PCT/JP00/03482

# 日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

23.06.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.



出願年月日
Date of Application: 1999年 5月31日

出願番号
Application Number: 平成11年特許願第152057号 09/980093

出願人
Applicant (s): 松下電器産業株式会社

09/980093

REC'D 04 AUG 2000
WIPO PCT

09/980093

## PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 8月18日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特2000-3064381

【書類名】　特許願

【整理番号】　2037810076

【提出日】　平成11年 5月31日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/78

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　柏　浩

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100081813

【弁理士】

【氏名又は名称】　早瀬　憲一

【電話番号】　06(6380)5822

【手数料の表示】

【予納台帳番号】　013527

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9600402

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ記録媒体、及びデータ管理システム

【特許請求の範囲】

【請求項１】　コンテンツ記録用または再生用のデータ記録媒体において、

上記データ記録媒体に、

著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したことを特徴とするデータ記録媒体。

【請求項２】　請求項１記載のデータ記録媒体において、

上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、

上記自立型再生履歴管理機能付き回路は、上記ディスクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのディジタル形式での出力回数を制限するコンテンツ出力管理部とを有することを特徴とするデータ記録媒体。

【請求項３】　請求項２記載のデータ記録媒体において、

上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、

上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コンテンツのタイトル単位または任意のデータサイズ単位でのディジタル形式での出力回数を制限するものであることを特徴とするデータ記録媒体。

【請求項４】　請求項２記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのディジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのディジタル形式での出力を抑制するものであることを特徴とするデータ記録媒体。

【請求項５】　請求項４記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で同時に複数

の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのディジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのディジタル形式での出力を計数するものであることを特徴とするデータ記憶媒体。

【請求項６】　請求項１記載のデータ記録媒体において、

上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報を記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するものであることを特徴とするデータ記憶媒体。

【請求項７】　請求項６記載のデータ記録媒体において、

上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知することを特徴とするデータ記憶媒体。

【請求項８】　コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、

上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、

記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、

上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生することを特徴とするデータ管理システム。

【請求項９】　請求項８記載のデータ管理システムにおいて、

上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化装置と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コ

ンテンツの復号化の可否を判定することを特徴とするデータ管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はデータ記録媒体、及びデータ管理システムに関し、特にディジタルコピーに対するコンテンツの著作権保護を向上させるための技術に関するものである。

【０００２】

【従来の技術】

現在、コンテンツのディジタル化が進んでいるが、ディジタルによるコピーは劣化が無いことから、ディジタルコピーによる著作権保護が問題になっている。そのため、図４４に示すように、Ｆｒｅｅ、Ｎｅｖｅｒ　Ｃｏｐｙ、Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ、Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙの４つの状態により著作権保護情報を示すＣＧＭＳ(Copy Generation Management System)方式が提案されている。図４５はこのＣＧＭＳ方式により著作権保護を制御するディジタル出力を備えた再生装置５０４であり、図４５において、５００は、例えば、ＣＤ－ＲＯＭのようなディスクメディア、５０４は再生装置である。そして、再生装置５０４は、ディスクメディアから、例えば光ピックアップなどを用いて読み出された信号を処理するための再生信号処理回路５０１，再生信号を出力するためのディジタルインターフェース、上記再生信号処理回路５０１，ディジタルインターフェース５０３の動作を制御するためのＣＰＵ５０２から構成されている。

【０００３】

以下、上記従来の著作権保護を制御するディジタル出力を備えた再生装置５０４におけるＣＧＭＳ方式を用いたコンテンツのディジタル出力の制御について説明する。

まず、ディスクメディア５００に付加されているＣＧＭＳ情報は、再生信号処理５０１からＣＰＵ５０２に転送される。ＣＰＵ５０２は、ＣＧＭＳ情報に応じてディスクメディア５００の再生データの、ディジタルインターフェース５０３からのディジタル出力を以下のように制御する。

１．ＣＧＭＳが「Ｆｒｅｅ」の場合は、ディジタルインターフェース５０３からの再生データ出力を常時認める。

２．ＣＧＭＳが「Ｎｅｖｅｒ　Ｃｏｐｙ」の場合は、ディジタルインターフェース５０３からの再生データ出力を認めない。

３．ＣＧＭＳが「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」の場合は、ディジタルインターフェース５０３からの再生データ出力を１回だけ認める。

４．ＣＧＭＳが「Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙ」の場合は、ディジタルインターフェース５０３からの再生データ出力を認めない。

【０００４】

ここで、ディジタルインターフェース５０３に記録装置が接続され、「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」のデータを記録装置に出力する場合は、記録装置側で「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」となっている情報を「Ｎｏ　Ｍｏｒｅ　Ｃｏｐｙ」に書き換えて記録媒体に新たにデータを記録・管理するように構成されている。

【０００５】

また、上記構成では、コンテンツのＣＧＭＳ情報が「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」の場合、元ディスクメディアからの１回コピーが際限なく可能であるため、これに鑑みて、コピー回数を制限するための情報をディスクメディア５００面上に記録可能な管理情報領域５０５を設け、該情報が所定値になったらコピー禁止となるように再生装置を構成しておき、「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」のコンテンツのコピーを行う毎にコピー回数を書き換え、所定値と一致したら、それ以降の元ディスクメディアからのコピーを抑制する方式も考えられる。

【０００６】

【発明が解決しようとする課題】

従来のデータ記録媒体、及びデータ管理システムは以上のように構成されており、ＣＧＭＳ情報を有する記録媒体から複製されたコンテンツは、これを用いてさらにコンテンツの複写を行うことができないように、記録媒体に記録時にＣＧＭＳ情報の書き換えを行っているが、上記従来の構成では、例えば、ＣＧＭＳ情報が「Ｏｎｅ　Ｍｏｒｅ　Ｃｏｐｙ」である場合は、当該記録媒体に対するディ

ジタルコピー回数の制限ができないため、コンテンツのディジタルコピーによる著作権の侵害を効果的に防止することができないという問題点を有していた。

【０００７】

また、ディスクメディアの所定領域にコピー回数を管理するための書き換え可能な領域を設けたとしても、ディスクメディアに形成されたピット形状を物理的にコピーする、いわゆる、スタンプコピーなどによる著作権の侵害を効果的に防止することができないという問題点があった。

【０００８】

本発明は、上記従来の問題点を解決するためになされたものであり、ディスクメディアにおける安全性の高い著作権管理を提供することを目的とする。

【０００９】

【課題を解決するための手段】

この発明の請求項１にかかるデータ記憶媒体は、コンテンツ記録用または再生用のデータ記録媒体において、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したものである。

【００１０】

また、この発明の請求項２にかかるデータ記憶媒体は、上記請求項１記載のデータ記録媒体において、上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、上記自立型再生履歴管理機能付き回路は、上記ディスクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのディジタル形式での出力回数を制限するコンテンツ出力管理部とを有するものである。

【００１１】

また、この発明の請求項３にかかるデータ記憶媒体は、上記請求項２記載のデータ記録媒体において、上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コン

テンツのタイトル単位または任意のデータサイズ単位でのディジタル形式での出力回数を制限するものである。

【００１２】

また、この発明の請求項４にかかるデータ記憶媒体は、上記請求項２記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのディジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのディジタル形式での出力を抑制するものである。

【００１３】

また、この発明の請求項５にかかるデータ記憶媒体は、上記請求項４記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で同時に複数の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのディジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのディジタル形式での出力を計数するものである。

【００１４】

また、この発明の請求項６にかかるデータ記憶媒体は、上記請求項１記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報を記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するものである。

【００１５】

また、この発明の請求項７にかかるデータ記憶媒体は、請求項６記載のデータ記録媒体において、上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知するものである。

【００１６】

また、この発明の請求項８にかかるデータ管理システムは、上記コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生するものである。

【００１７】

また、この発明の請求項９にかかるデータ管理システムは、上記請求項１０記載のデータ管理システムにおいて、上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化処置と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コンテンツの復号化の可否を判定するものである。

【００１８】

【発明の実施の形態】

以下、本発明のよるデータ記録媒体、及びデータ管理システムについて、図面を参照しながら説明する。

実施の形態１.

図１は本発明の実施の形態１によるデータ記録媒体であるディスクメディア１００の概念的な構成図であり、図１において、９０はセンタホール、１００は、例えば、ＤＶＤ－ＲＡＭなどのポリカーボンで構成されたディスクメディア、１０１は記憶素子として不揮発性半導体チップなどを含む半導体チップ（自立型再生履歴管理機能付き回路）、１０２はデータ領域、１０３はディスクメディア１００を後述する回転ドライブに固定するためのクリッピング領域、１０４はディスクメディア１００の記録データ１０２の管理情報を記録したＴＯＢ（Table of contents）領域である。

なおここでは、半導体チップは１個であるが、例えば２個ならばセンタホール９０を挟んで対称になる様にすることで複数ある場合におけるバランスを取る様に配置してもよい。

【００１９】

図２は上記ディスクメディア１００に搭載された半導体チップ１０１と電気的な信号の接続を行うためのディスクメディアに設けられるワイヤー線の配置の一例を示した図である。図において、１０５はクリッピング領域１０３に設けられたワイヤー配線であり、ディスクメディア１００の外周側から双方向の信号線であるデータ線、電源を供給する電源線、半導体チップ１０１駆動時のクロックを供給するクロック線、接地電位を供給するためのGND線からなり、この順で円周状に配置されている。

なお、図２ではディスクメディア１００の片側上面にのみワイヤー配線を配置しているが、両面に配置するようにしてもよい。

【００２０】

図３（ａ），（ｂ）は、上記構成を有するディスクメディア１００を用いて記録／再生を行う記録再生装置２００とディスクメディア１００に設けられたワイヤー配線１０５との接続を行う際の一部平面図、および断面図を示し、図において１０６はディスクメディア１００を配置するトレイ、１０７はディスクメディア１００を固定するクリッピング、１０８はクリッピング１０７のディスクメディア１００との当接面に、ディスクメディア１００のワイヤー配線１０５に対応して設けられたワイヤー配線である。すなわち、ワイヤー配線１０８は、ディスクメディア１００の外周側よりデータ線，電源線，クロック線，ＧＮＤ線が同心円上に配置されている。なお、ワイヤー配線１０８のうちのデータ線は、後述するメディア管理部に接続されている。

また、１０９はディスクメディア１００を回転させるためのスピンドルモータ、２０８はディスクメディア１００のデータ領域１０２に形成されたピットを読み出すための光ピックアップである。

【００２１】

以上のような構成を用い、ディスクメディア１００をトレイ１０６に搭載され

ると、トレイ１０６は記録再生装置２００内部に収納され、ディスクメディア１００はクリッピング１０６とスピンドルモータ１０９により上下からクランピングされ、スピンドルモータ１０９により回転し、光ピックアップ２０８によってディスクメディア１００のデータ領域１０２をアクセスし、後述する暗号部と、記録／再生するデータの通信を行う。上記クリッピング１０７がディスクメディア１００を固定する際に、ディスクメディア１００に配置されたワイヤー配線が接触することでデータ線を通じて記録再生装置２００とディスクメディア１００上の半導体チップ１０１がデータ通信を行うことができる。

【００２２】

次に動作について説明する。

まず、記録動作について説明する。

ディスクメディア１００にコンテンツを暗号化して記録する場合、図４に示すように、半導体チップ１０１は、双方向の通信ポートであるＩ／Ｏ１１０、データ信号，制御信号のコントロールおよび演算を行うＣＰＵ１１１（コンテンツ出力管理部）、記録データの管理情報を保持する、例えば、ＥＰＲＯＭやＥＥＰＲＯＭなどの不揮発性メモリで構成された記憶部を有している。

【００２３】

表１は上記記憶部１１２に保持された情報の内容を示し、１１４はタイトル、１１５はタイトル単位で暗号化している場合の復号鍵を保持する復号鍵部、１１６はタイトル単位で、記録データのディジタル出力された回数を制限する情報であるディジタル出力制限回数情報である。

【００２４】

【表１】

| | | |
|---|---|---|
| 114 | タイトル | プログラムA ・・ |
| 115 | 復号鍵部 | 鍵A ・・ |
| 116 | ディジタル出力制限回数情報 | 5 ・・ |

図５はディスクメディア１００にデータを記録または記録データを再生するための、図３に示したところの記録再生装置２００のブロック構成図であり、図５において、２０１は信号処理部、２０２はディスクメディアへのデータのリード／ライトを管理するためのメディア管理部、２０３は記録再生装置２００におけるデータ信号，制御信号をコントロールするＣＰＵ、２０４は記録再生装置２００と接続ケーブル２１３で接続された外部機器である外部記録再生装置２１２とのデータの双方向通信を行うためのディジタルインターフェース、２０５はディジタルデータをアナログに変換して出力するＤ／Ａ変換器である。

【００２５】

また、２０６はユーザが記録再生装置２００の操作を行うためのユーザ設定部、２０７は記録再生装置２００の動作を表示するユーザインターフェースでもある表示部、２０８はディスクメディア１００にデータを記録または再生する光ピックアップ、２０９はアナログデータをディジタルデータに変換するＡ／Ｄ変換器、２１０は暗号部２１０で用いる鍵を発生する乱数部である。

【００２６】

ここで、半導体チップ１０１のディジタル出力制限回数情報１１６のデータは設定しない場合は、「０」とし、設定した場合においてディジタルコピーを行う毎にカウントダウンして、その値が「１」となった場合にディジタルコピー不許可とするものとし、例えば、１回だけディジタルコピーを許可する場合には上記値を「２」に設定するものとして説明する。また、ディスクメディア１００におけるコンテンツの記録または再生は、タイトル単位で行うこととする。

図６に示すように、ステップＺ１、ステップＺ３は記録再生装置２００で行い、ステップＺ２は半導体チップ１０１で行い、ステップＺ１～ステップＺ３の手順で行われる。

【００２７】

すなわち、図７に示すステップＺ１では、ステップＡ２０１において記録再生装置２００に、ディスクメディア１００を図３で示したように配置した時に、ＣＰＵ２０３が、光ピックアップ２０８がディスクメディア１００のＴＯＢ領域１０４をアクセスすることで、ディスクメディア１００における，ユーザが記録し

たデータのタイトルと配置、及び空領域などを検出した上で、タイトルを表示部２０７に表示する。

【００２８】

次いで、ステップＡ２０２において、ユーザが記録するコンテンツデータのタイトル、ディジタル出力制限回数情報、コンテンツの暗号化の有無をユーザ設定部２０６に設定（ここでは、タイトル：プログラムＡ、ディジタル出力制限回数情報：５、暗号化：有り）する。

ステップＡ２０３において、ＣＰＵ２０３はユーザ設定部２０６に設定された情報をもとに、タイトル，ディジタル出力制限回数情報をメディア管理部２０２に転送し、ステップＡ２０４において、アナログデータであるプログラムＡは、Ａ／Ｄ変換器２０９に入力され、ここでディジタルに変換され、さらに、信号処理部２０１に伝送され、ここでプログラムＡは記録フォーマット化され、そして暗号部２１０に伝送され、暗号部２１０において、鍵を用いてプログラムＡを暗号化して光ピックアップ２０８に伝送し、ＣＰＵ２０３の制御により光ピックアップ２０８からディスクメディア１００の記録データ領域１０２の空領域に上記暗号化されたプログラムＡを記録するとともに、記録したデータのタイトルとディスクメディア１００におけるデータの配置をＴＯＢ領域１０４に記録する。

ステップＡ２０５において、メディア管理部２０２はデータ線を介して登録コマンド，タイトル（プログラムA），ディジタル出力制限回数情報（５），鍵Ａを半導体チップ１０１に送信する。

【００２９】

ステップＡ２の処理である図８では、ステップＡ２０８において、登録コマンド，タイトル（プログラムA），ディジタル出力制限回数情報（１０），鍵Ａを、Ｉ／Ｏ１１０で受信しする。

ステップＡ２０９において、ＣＰＵ１１１はＩ／Ｏ１１０の受信した登録コマンドにより、ステップＡ２０７の受信情報を記憶部１１２に伝透し、表１にあるように記憶する。

そして、ステップＡ２１０において、記憶後通信終了をメディア管理部２０２に送信する。

ステップＡ３の処理である図９では、ステップＡ２１３において通信終了を受信しディスクメディア１００への設定情報の記憶動作が終了する。

【００３０】

以上のようにして、ディスクメディアへのコンテンツの書き込みが行われる。

次に、コンテンツを暗号化して記録しているディスクメディア１００を記録再生装置２００において再生する動作について図１０～図１４のフローチャートを参照しつつ説明する。

【００３１】

図１０に示すように、ステップＡ１，ステップＡ３は記録再生装置２００で行い、ステップＡ２，ステップＡ４は半導体チップ１０１で行い、ステップＡ１～ステップＡ４の手順で行われる。

【００３２】

まず、ステップＡ１の処理である図１１では、ステップＡ４０１において、記録再生装置２００にディスクメディア１００を図３に示したように配置した時に、ＣＰＵ２０３が、光ピックアップ２０８がディスクメディア１００のＴＯＢ領域１０４をアクセスすることで、ディスクメディア１００における，ユーザが記録したデータのタイトルと配置、及び空領域などを検出した上で、タイトルを表示部２０７に表示する。

【００３３】

次いで、ステップＡ４０２において、ユーザ設定部２０６に、ユーザが再生したいタイトルをディジタルインターフェース２０４から接続ケーブル２１３を介して外部記録再生装置２１２に対して出力するか否かの有無を、ユーザ設定部２０６を介してＣＰＵ２０３に設定（タイトル：プログラムＡ、ディジタル出力：有とする）する。

ステップＡ４０３において、ＣＰＵ２０３は、再生のスタートを示すスタートコマンド，再生したいタイトル，ディジタル出力の有無の情報を、メディア管理部２０２よりデータ線１０８，１０５を介して半導体チップ１０１に送信する。

【００３４】

ステップＡ２の処理である図１２では、ステップＡ４０６において、半導体チ

ップ１０１はステップＡ４０２で設定された情報をＩ／Ｏ１１０で受信し、ＣＰＵ１１１がスタートコマンドを確認し、その後、ステップＡ４０７において、ディジタル出力の有無を確認する。ここで、ディジタル出力が無い場合（ｎｏ）には、ステップＡ４０９に進んでタイトル（プログラムＡ）に応じて記憶部１１２の復号鍵部１１５より選択した復号鍵（鍵Ａ）を記録再生装置２００に送信する。

【００３５】

一方、上記ステップＡ４０７において、ディジタル出力有りの場合（ｙｅｓ）には、ステップＡ４０８に進んで、半導体チップ１０１のディジタル出力制限回数情報１１６と「２」とを比較してディジタル出力制限回数情報１１６が「２」以上の場合（ｙｅｓ）に、スヂップＡ４０９においてタイトル（プログラムＡ）に応じて記憶部１１２の復号鍵部１１５より選択した復号鍵（鍵Ａ）を記録再生装置２００に送信する。

ステップＡ４０８において、ディジタル出力制限回数情報１１６が「２」より小さい場合（ｎｏ）には、ステップＡ４１０において、コンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを記録再生装置２００に送信し、ステップＡ４１１において通信を終了する。

【００３６】

ステップＡ３の処理である図１３では、ステップＡ４１４において、ステップＡ４０９における復号鍵の受信、またはステップＡ４１０における再生不許可コマンドを受信し、ステップＡ４１５において、再生不許可コマンドが確認され、再生不許可コマンドの場合（ｙｅｓ）に、ステップＡ４１６に進んで、表示部２０７において視覚または聴覚的にステップＡ４０２における設定情報の変更を促す。

【００３７】

ここで、ステップＡ４０３終了以降は、ステップＡ４０２の設定情報は変更できず、変更の場合は、設定情報を消去してステップＡ４０２から設定やり直すものとする。これにより、例えば、ステップＡ４０２でディジタル出力を「無」と設定してステップＡ４０２終了後に、ディジタル出力を「有り」とすることでス

テップＡ４０８よりにディジタル出力が不可能なコンテンツの不正なディジタル出力を防ぐことが可能である。

【００３８】

一方、上記ステップＡ４１５において、再生不許可コマンドではない場合（ｎｏ）には、ステップＡ４１７に進んでステップＡ４０２で設定されたディジタル出力の有無を確認し、「有り」の場合（ｙｅｓ）にはステップＡ４１８に進んでステップＡ４０２で設定されたタイトル（プログラムＡ）のコンテンツをステップＡ４１４で受信した復号鍵（鍵）を用いて再生し、復号化データをディジタルインターフェース２０４よりディジタル形式で出力し、ステップＡ４１９において、再生か終了したら再生終了を半導体チップ１０１に送信する。

【００３９】

上記ステップＡ４１７において、ステップＡ４０２で設定されたディジタル出力の有無を確認し、これが「無し」の場合（ｎｏ）には、ステップＡ４２０に進んでステップＡ４０２で設定されたタイトルのコンテンツ（プログラムＡ）を、ステップＡ４１４で受信した復号鍵（鍵Ａ）を用いて復号化してＤ／Ａ変換器２０５からのアナログ形式で再生する。

【００４０】

ステップＡ４の処理である図１４では、ステップＡ４２２において半導体チップ１０１は再生終了をＩ／Ｏ１１０で受信し、ＣＰＵ１１１が再生終了を確認したらステップＡ４２３において記憶部１１２のディジタル出力制限回数情報１１６から「１」を引いた回数「５－１＝４」をディジタル出力制限回数情報１１６を更新することで記録してコンテンツの再生が終了する。

【００４１】

以上のように、本実施の形態によれば、コンテンツ記録媒体であるディスクメディア１００に半導体チップ１０１を設け、半導体チップ１０１にディジタル出力回数を制限するための情報を保持させて管理するようにしたので、コンテンツのディジタルコピー等のディジタル出力の回数を制限でき、また、スタンプコピーのような方法で物理的にコンテンツ記憶領域をコピーしても、半導体チップ１０１はコピーされず、しかもコンテンツは半導体チップ１０１内に格納された鍵

でしか符号化できないように暗号化されているので、コンテンツの内容が再生可能な状態で外部に取り出されることがない。

【００４２】

さらに、ステップＡ４２３においてコンテンツの再生終了を確認した上で、ディジタル出力制限回数情報を更新するようにしているため、何らかのトラブルなどで再生途中でディジタル出力が停止した場合においても、コンテンツのディジタル出力を保証することができる。

【００４３】

実施の形態２．

次に本発明の実施の形態２によるデータ記録媒体、及びデータ管理システムについて説明する。上記実施の形態１では、ディジタルインターフェースが１つである場合について説明したが、本実施の形態２では、複数のディジタル入出力口を備えた再生動作を用いる場合について説明する。

【００４４】

図１５は半導体チップ１０１ａの構成を示す図であり、図において、１１３は記録データを再生する装置の外部にディジタル出力する場合に、外部にディジタル出力する数を保持するためのディジタル出力数保持部（出力経路数記憶部）である。ここで、その他、図４と同一符号は同一または相当部分を示すものとする。

【００４５】

図１６は複数のディジタル入出力口備え、ディスクメディア１００の記録データを再生可能な図３における動作を保有する記録再生装置のブロック図であり、図において、３００は記録再生装置、３０１はディジタルインターフェース（Ａ）、３０２は複数のディジタル出力口を有するディジタルインターフェース（Ｂ），３０３はハードディスク（ＨＤＤ）装置（Ａ）、３０４はハードディスク（ＨＤＤ）装置（Ｂ）である。その他、図５と同一符号は同一または相当部分を示すものとする。

【００４６】

以上に構成された再生装置４００について図１８～２１のフローチャートを参

照しつつ説明する。

ディスクメディア１００におけるコンテンツを再生するには、図１７に示すように、ステップＢ１とステップＢ３は記録再生装置３００で行い、ステップＢ２とステップＢ４を半導体チップ１０１ａで行い、ステップＢ１～ステップＢ４の手順で行う。

【００４７】

ステップＢ１の処理である図１８では、ステップＡ６０１において、記録再生装置４００にディスクメディア１００を図３のように配置した時に、ＣＰＵ２０３は光ピックアップ２０８がＴＯＢ領域１０４をアクセスすることで、ディスクメディア１００における，ユーザが記録したデータのタイトルと配置、および空領域等を認識した上で、タイトルを表示部２０７に表示する。

【００４８】

次いで、ステップＢ６０２において、ユーザ設定部２０６にユーザが再生したいタイトルをディジタルインターフェースＡ３０１，３０２から、接続ケーブル２１３を介して外部記録再生装置２１２、ＨＤＤ装置Ａ３０３，Ｂ３０４に対してディジタル出力する場合に選択し、ディジタル出力する数をユーザ設定部２０６を介してＣＰＵ２０３に設定（タイトル：プログラムA、ディジタル出力：３とする）し、ステップＢ６０３において、再生のスタートを示すスタートコマンド、再生したいタイトル、ディジタル出力の数を半導体チップ１０１に透信する。ここで、ステップＢ６０２におけるディジタル出力がない場合は「０」として説明する。

【００４９】

ステップＢ２の処理である図１９では、ステップＢ６０６において、ステップＢ６０２で設定された情報を受信し、スタートコマンドを確認した後、ステップＢ６０７においてディジタル出力数を「１」と比較することで、ディジタル出力の有無を検出している。そして、ステップＢ６０７において、ディジタル出力数が「０」の場合（ｎｏ）には、ディジタル出力を「無い」としてステップＢ６１４に進んで、タイトルに応じて復号鍵部１１５より選択した復号鍵（鍵Ａ）を記録再生装置３００に送信する。

一方、ステップＢ６０７においてディジタル出力数が「０」以外の場合（ｙｅｓ）には、ディジタル出力を「有り」としてステップＢ６０８に進んでディジタル出力制限回数情報１１６と「２」とを比較することでディジタル出力が可能かを検出する。

【００５０】

次いで、ステップＢ６０８において、ディジタル出力制限回数情報１０７が「２」より小さい場合（ｎｏ）には、ステップＢ６１１に進んで、コンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを半導体チップ１０１に送信する。一方、上記ステップＢ６０８において、ディジタル出力制限回数情報１１６が「２」以上の場合（ｙｅｓ）にはステップＢ６０９を実行する。

【００５１】

上記ステップＢ６０９においては、ディジタル出力数と「２」とを比較して、ディジタル出力数が「２」未満、つまり、「１」以下の場合（ｎｏ）には、ステップＢ６１３においてディジタル出力数をディジタル出力数保持部１１３に設定し、ステップＢ６１４においてタイトル（プログラムＡ）に応じて復号鍵部１１５より選択した復号鍵（鍵Ａ）を記録再生装置３００に送信する。

【００５２】

上記ステップＢ６０９においてディジタル出力数が２より大きい場合（ｙｅｓ）にはステップＢ６１０に進んで、ここで、ディジタル出力制限回数情報１１６－ディジタル出力数と、「２」とを比較して、ディジタル出力制限回数情報１１６－ディジタル出力数が「２」よりも小さい場合（ｙｅｓ）にステップＢ６１１においてコンテンツを再生するための復号鍵の送信を拒否する再生不許可コマンドを半導体チップ１０１に送信し、ステップＢ６１２において通信を終了する。

【００５３】

一方、上記ステップＢ６１０においてディジタル出力制限回数情報１１６－ディジタル出力数が「１」以上の場合（ｎｏ）には、ステップＢ６１３に進んでディジタル出力数をディジタル出力数保持部１１３（３）に設定し、ステップＢ６１４においてタイトル（プログラムＡ）に応じて復号鍵１１５より選択した復号鍵（鍵Ａ）を記録再生装置３００に送信する。

【００５４】

ステップＢ３の処理である図２０では、ステップＢ６１６において、ステップＢ６１１の再生不許可コマンド、またはステップＢ６１４の復号鍵を受信し、ステップＢ６１７において、上記受信したものが再生不許可コマンドか否かを確認し、これが再生不許可コマンドであった場合（ｙｅｓ）には、ステップＢ６１９に進んで、表示部２０７において視覚または聴覚的にステップＢ６０２における設定情報の変更を促す。

【００５５】

一方、上記ステップＢ６１７において、受信したものが再生不許可コマンドでないと判定された場合（ｎｏ）には、ステップＢ６２０に進んで、ディジタル出力数と「１」とを比較することで、ディジタル出力の有無を検出する。

ステップＢ６２０において、ディジタル出力数が「１」の場合（ｎｏ）には、ディジタル出力を「無い」としてステップＢ６２３において、ステップＢ６０２で設定されたタイトル（プログラムＡ）のコンテンツをステップＢ６１６で受信した復号鍵（鍵Ａ）を用いてＤ／Ａ変換器２０５からのアナログ出力のみを再生する。

【００５６】

一方、上記ススステップＢ６２０において、ディジタル出力数が「１」以外の場合（ｙｅｓ）には、ディジタル出力を「有り」として、ステップＢ６０２で設定されたタイトル（プログラムＡ）のコンテンツを、ステップＢ６１６で受信した復号鍵（鍵Ａ）を用いて再生し、ディジタルインターフェース（Ａ）３０１、またはディジタルインターフェース（Ｂ）３０２よりディジタル形式で出力し、ステップＢ６２２において再生が終了したら再生終了を半導体チップ１０１ａに送信する。

【００５７】

ステップＢ４の処理である図２１では、ステップＢ６２５において、再生終了の確認行い、再生終了ならばステップＢ６２６に進んで、ディジタル出力制限回数情報１１６からディジタル出力数保持部１１３（３）を引いた回数をディジタル出力制限回数情報１１６（２）を更新することで記憶させ、コンテンツの再生

を終了する。

【００５８】

このように本実施の形態２によれば、複数のディジタル出力口を備えた再生装置において、半導体チップ１０１ａに、ディジタル出力する数を保持する機能を持たせ、ディジタルコピー終了後に、ディジタル出力制限回数情報１１６からディジタル出力数保持部１１３の値を減算することで、複数のディジタル出力を用いて、再生したコンテンツを同時にディジタルコピー等する場合におけるコピー回数の制限を行うことができる。

【００５９】

実施の形態３．

次に本発明の実施の形態３によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態３では、上記実施の形態１または２において、半導体チップ１０１ｂが、ユーザの個人情報（パスワード）を用いた本人認証することでディスクメディアの再生を許可する機能を付加したものである。なお、ここでは、実施の形態１に本実施の形態３の機能を適用したものを例にとって説明する。

【００６０】

図２２は本実施の形態３における半導体チップ１０１ｂの構成を示すブロック図であり、図において、１１７は本人認証を目的とするパスワードを保持する個人情報保持部（個人情報記憶部）である。その他の部分については、図４と同一であるのでここでは、その説明については省略するものとする。

【００６１】

以上のように構成された本実施の形態３の動作について図２３～２７のフローチャートを参照しつつ説明する。なお、ここでは、個人情報保持部１１７が「０」の値の場合に個人情報が登録されていないものとし、ディスクメディア１００は記録または再生しようとする装置に配置され、電源が投入された時点で、半導体チップ１０１ｂのＣＰＵ１１１が個人情報保持部１１７を確認し、個人情報が設定（０以外に）されている場合に、記録再生装置２００からの入力された個人情報と一致しなければ記憶部１１２へのアクセスを制限するものとして説明する

【００６２】

まず、本人を認証するための個人情報を半導体チップ１０１に記録再生装置２００によって登録する動作について説明する。

図２３に示すように、ステップＣ１、ステップＣ３は記録再生装置２００で行い、ステップＣ２とステップＣ４を半導体チップ１０１ｂで行い、ステップＣ１～ステップＣ５の手順で行う。

ステップＣ１の処理である図２４では、ステップＣ８０１において、ディスクメディア１００が記録再生装置２００に配置されることで、ＣＰＵ２０３はディスクメディア１００における個人情報の登録の有無を確認する個人情報確認コマンドを送信する。

【００６３】

次いで、ステップＣ２の処理である図２５では、ステップＣ８０４において、個人情報確認コマンドを受信し、ＣＰＵ１１１ｂは個人情報確認コマンドに基づきステップＤ８０５において個人情報の有無を確認するために、個人情報保持部１１７と「０」とを比較して個人情報保持部１１７が「０」の場合（ｎｏ）には、「個人情報無し」としてステップＣ８０７に進んで個人情報無しコマンドを送信する。一方、上記ステップＣ８０５において個人情報保持部１１７が「０」では無い場合（ｙｅｓ）には、「個人情報有り」としてステップＣ８０６に進んで個人情報有りコマンドを送信する。

【００６４】

ステップＣ３の処理である図２６では、ステップＣ８１１において個人情報有りコマンド、または個人情報無しコマンドを受信し、ＣＰＵ２０３はステップＣ８１２において、個人情報無しコマンドか否かを確認し、個人情報が無しコマンドが検出された場合（ｙｅｓ）には、ステップＣ８１３に進んで再生動作を行うか、または個人情報を登録するための登録コマンドと登録する個人情報をユーザ設定部２０６より入力して半導体チップ１０１ｂに送信する。なお、上記ステップＣ８１２において個人情報が無しコマンド以外が検出された場合（ｎｏ）の動作については後述するの本人認証の動作で説明する。

ステップＣ４の処理である図２７では、ステップＣ８１７において登録コマンドと登録する個人情報を受信し、ＣＰＵ１１１ｂは登録コマンドに基づき、ステップＣ８１８において個人情報を個人情報保持部１１７に記憶する。

【００６５】

次に本人認証を行うための個人情報が半導体チップ１０１ｂに登録さている場合における、記録再生装置２００の動作を図２８～３１を参照しつつ説明する。

図２８に示すように、ステップＣ１とステップＤ３とステップＤ５は記録再生装置２００で行い、ステップＣ２とステップＤ４を半導体チップ１０１ｂで行い、ステップＤ１～ステップＤ５の手順で行う。なおここでは、図２３～２７と同一ステップ名は同一処理としてその説明を省略するものとする。

【００６６】

ステップＤ３の処理である図２９では、ステップＤ１０１１において個人情報有りコマンド、または個人情報無しコマンドを受信し、次いで、ＣＰＵ２０３はステップＤ１０１２において、個人情報無しコマンドか否かを確認し、個人情報が無しコマンド以外の場合（ｎｏ）には、ステップＤ１０１４において表示部２０７に個人情報の入力を促し、個人情報が入力された時点でステップＤ１０１５において、個人情報の確認命令である個人情報コマンドと入力個人情報とを半導体チップ１０１ｂに送信する。

【００６７】

次いで、ステップＤ４の処理である図３０では、ステップＤ１０１８において、個人情報コマンドと入力個人情報とを受信し、ＣＰＵ１１１ｂは個人情報コマンドに基づいてステップＤ１０１９において、個人情報保持部１１７と入力個人情報とを比較し、これらが一致した場合（ｙｅｓ）には、ステップＤ１０２０に進んで本人認証成立を伝える継続コマンドを送信し、逆に、不一致の場合（ｎｏ）にはステップＤ１０２１に進んで通信終了を送信する。

【００６８】

ここで、ステップＤ１０１９において（ｙｅｓ）の場合にユーザの本人認証が成立し、ＣＰＵ１１１ｂは、以後、記憶部１１２へアクセスを行うように動作することで、ディスクメディア１００への記録または再生動作が可能になる。

【００６９】

ステップＤ５の処理である図３１では、ステップＤ１０２４において継続コマンド、または通信終了を受信し、ステップＤ１０２５においてＣＰＵ２０３は継続コマンドか否かの確認を行い、ここで維続コマンドの場含（ｙｅｓ）であると判定された場合には、ステップＤ１０２６に進んで、ディスクメディア１００への記録または再生動作や、個人情報保持部１１７の情報を消去するための命令である消去コマンドの発行や、登録されている個人情報を変更するための登録コマンド等を送信することが可能となる。

【００７０】

一方、上記ステップＤ１０２５において、継続コマンドでないと判定された場合（ｎｏ）には、ステップＤ１０２７に進んで通信を終了する。

【００７１】

なお、上記個人情報保持部１１７に、複数の個人情報を備え、ユーザが個人情報保持部１１７の自分の個人情報を選択し、上記動作を複数回行うように構成することも可能である。

また、半導体チップ１０１ｂの記憶部１１２に登録しているタイトル単位で本人認証情報を設定し、本人認証が成立したときのみ再生可能となるように構成してもよい。

【００７２】

このように本実施の形態３によれば、ディスクメディア１００の半導体チップ１０１ｂに、ユーザの個人情報（パスワード）を記憶し、メディア再生時に認証を行うようにすることで、ディスクメディア側でユーザの識別が可能となり、第３者によるディスクメディア１００の不正コピー等の行為を防止することができ、コンテンツの安全性を強固なものとすることができる。

【００７３】

実施の形態４．

次に本発明の実施の形態４によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態４では、上記実施の形態３において、半導体チップの個人情報保持部に個人情報が設定されている場合、本人認証への不正動作を

検出する機能を付加したものである。すなわち、図３２は本実施の形態４における半導体チップ１０１ｃの構成を示すブロック図であり、図において、１１８は個人情報（パスワード）の確認が一致しなかった回数を保持するための不正回数保持部（不一致回数保持部）である。その他の部分については図２２で示したものと同一であるので、ここではその説明は省略する。

なお、ここでは、不正回数保持部１１８には「０」以外の任意の値が設定されており、記憶された値をクリアすることで任意の値が設定されるものとし、不正回数保持部１１８に「０」が保持されると不正アクセスが検出されたものとして説明する。

【００７４】

以下、本人認証するための個人情報が半導体チップ１０１ｃに登録さている場合に、例えば、個人情報を解析する目的など、不正なアクセスを検出する動作を中心に、図３３から３５を参照しつつ説明する。

図３３に示すように、ステップＣ１とステップＤ３とステップＥ５は記録再生装置２００で行い、ステップＣ２とステップＥ４を半導体チップ１０１で行い、ステップＤ１～ステップＥ５の手順で行う。ここで、図２８と同一ステップ名は同一処理としてその説明は省略する。

【００７５】

まず、ステップＥ４の処理である図３４では、ステップＥ１１０１において、個人情報コマンドと入力個人情報とを受信する。

次いで、ＣＰＵ１１１ｃは、ステップＥ１１０２において、不正回数保持部１１８の記憶内容と「０」とを比較し、不正回数保持部１１８の記憶内容が「０」の場合（ｙｅｓ）には、ステップＥ１１０３に進んで不正行為があったとして不正アクセスコマンドを記録再生装置２００に送信する。

【００７６】

一方、上記ステップＥ１１０２において、不正回数保持部１１８の記憶内容が「０」以外の場合（ｎｏ）には、ステップＥ１１０４に進んで、ＣＰＵ１１１ｃは個人情報コマンドに基づいて、個人情報保持部１１７と入力個人情報とを比較し、その結果が一致した場合（ｙｅｓ）には、ステップＥ１１０５に進んで不正

回数保持部１１８をクリアして「０」以外の所定値を設定し、ステップＥ１１０６において、本人認証成立を伝える継続コマンドを送信する。一方、上記ステップＥ１１０４において、不一致の場合（ｎｏ）にはステップＥ１１０７に進んで不正回数保持部１１８に記憶された値から「１」を減算した結果を不正回数保持部１１８として保持し、ステップＥ１１０８において通信終了を記録再生装置２００に送信する。

【００７７】

上記ステップＥ１１０５を実行することで、不正回数保持部１１８に設定されている値が「０」になる前に本人認証が成立すれば、不正回数保持部１１８がクリアされて所定値にもどる。これにより本人の誤入力などによって不正回数が記録しても、再度、正しい入力を行うことで上記誤入力による不正回数がカウントされ、誤入力による不正回数の蓄積によって不意にディスクメディアへのアクセスが不可能になることを防止している。また、本人以外の人物が不正な本人認証をしようと個人情報保持部１１７に記憶されていない情報を連続し入力した場合には、不正回数保持部１１８の値が「０」に近づいていき、不正回数保持部１１８が「０」になったときに不正アクセスがあったことが検出できる。

【００７８】

ステップＥ５の処理である図３５では、ステップＥ１１１１において、不正アクセスコマンド、または継続コマンド、または通信終了のいずれかを受信し、ステップＥ１１１２において、ＣＰＵ２０３は、上記受信した情報が、不正アクセスコマンドか否かの確認を行い、不正アクセスコマンドであった場合（ｙｅｓ）には、ステップＥ１１１３に進んで表示部２０７において視覚、または聴覚的に不正行為があったことの表示を行う。

【００７９】

一方、上記ステップＥ１１１２において、上記ＣＰＵ２０３が不正アクセスコマンド以外の情報を確認した場合（ｎｏ）には、ステップＤ１１１４に進んでＣＰＵ２０３は、その情報が継続コマンドか否かの確認をし、これが継続コマンドである場合（ｙｅｓ）には、ステップＥ１１１５に進んでディスクメディア１００への記録または再生動作、個人情報保持部１１７の情報を消去するための命令

である消去コマンドの発行、登録されている個人情報を変更するための登録コマンド等を送信することができる。

上記ステップＥ１１１４において、ＣＰＵ２０３が、継続コマンドでないと判定した場合（ｎｏ）には、ステップＥ１１１６に進んで通信を終了する。

【００８０】

このように本実施の形態４によれば、ディスクメディア１００の半導体チップ１０１ｃに不正アクセスした回数を記憶する機能を設けることで、例えば、第３者が悪意でディスクメディア１００に不正アクセスしたことをディスクメディア１００側で記録保持することができるため、ディスクメディア１００の正規の所有者に不正アクセスがあったことを警告することができる。

また、不正アクセスを検出した場合に、再生装置が、例えば、大きな音を発するなどで威嚇して不正行為を止めさせることも可能である。

【００８１】

実施の形態５．

次に本発明の実施の形態５によるデータ記録媒体、及びデータ管理システムについて説明する。本実施の形態５では、上述した各実施の形態において、暗号を用いた認証動作を行うようにしたものである。なお、ここでは実施の形態１において適用した場合を例にとって説明する。

図３６は本実施の形態５における半導体ＩＣ１０１ｄの構成を示すブロック図であり、図において、１１９は記録再生装置２００の暗号部２１０と同じ暗号アルゴリズムを有する暗号部、１２０は乱数を発生する乱数部、１２１はの暗号部１２０で用いる鍵配列の集合である鍵ボックス部である。その他の部分については、図４で示したものと同一であるため、ここではその説明は省略する。図３７は本実施の形態５における記録再生装置４００のブロック図であり、図３７において、２１４はディスクメディア１００に搭載された半導体チップ１０１ｄに含まれる鍵ボックス部１２１と同一機能を有する鍵ボックス部である。その他、図５と同一符号は同一または相当部分を示す。

表２は上記鍵ボックス部１２１、鍵ボックス部２１４に保持されている情報であり、表２において、１７００は鍵を選択するための鍵コード、１７０１は鍵コ

ード１７００に応じて選択される鍵である。

【表２】

| 1700 鍵コード | 1701 鍵 |
|---|---|
| 鍵コード1 | 鍵KC1 |
| 鍵コード2 | 鍵KC2 |
| ・ | ・ |
| ・ | ・ |

以上に構成されたディスクメディア１００の半導体チップ１０１ｄと記録再生装置４００における認証動作について図３８～４１のフローチャートを参照しつつ説明する。図３８に示すように、ステップＧ１、ステップＧ３、ステップＧ５は記録再生装置４００で行い、ステップＣ２、ステップＧ４を半導体チップ１０１で行いステップＧ１～ステップＧ５の手順で行う。

【００８２】

また、以降データの暗号化、または復号化においては下記のように示すものとする。

関数名＝Ｅ／Ｄ（Ａ，Ｂ）

Ｅ／Ｄ＝Ｅ：暗号化、Ｄ＝復号化とし、Ａは暗号化または復号化における鍵、Ｂは平文または暗号文を示している。

例えば、平文Ｂを鍵Ａにより暗号化して暗号文Ｃを生成するには、

Ｃ＝Ｅ（Ａ，Ｂ）

とする。復号化は、

Ｂ＝Ｄ（Ａ，Ｃ）

ステップＧ１の処理である図３９では、ステップＧ１８０１において認証スタートコマンドを半導体チップ１０１ｄに送信する。

【００８３】

ステップＧ２の処理である図４０では、ステップＧ１８０４において認証スタートコマンドを受信し、ＣＰＵ１１１ｄは認証スタートコマンドに基づいてステ

ップＧ１８０５において乱数部１２０により乱数を発生し、乱数ＲＸとし、ステップＧ１８０６において乱数ＲＸの並びを利用して、「鍵コード１」を生成し、鍵ボックス部１２１で鍵を選択して「鍵ＫＣ１」とし、ステップＧ１８０７において乱数ＲＸを「鍵ＫＣ１」を鍵として暗号部１２０で暗号化：Ｅ１＝Ｅ（ＫＣ１、ＲＸ）を実行しＥ１を作成し、ステップＧ１８０９においてＥ１と「鍵コード１」を記録再生装置４００に送信する。

【００８４】

ステップＧ３の処理である図４１では、ステップＧ１８１０においてＥ１と「鍵コード１」を受信し、ＣＰＵ２０３はステップＧ１８１１において、鍵ボックス部２１４で「鍵コード１」に対応した「鍵ＫＣ１」を選択し、ステップＧ１８１２において、Ｅ１を「鍵ＫＣ１」を鍵として暗号部１６００で復号化：Ｄ１＝Ｄ（ＫＣ１、Ｅ１）を実行してＤ１を作成する。

【００８５】

次いで、ステップG１８１４において、乱数部２１１で乱数を発生し、乱数の並びを利用して「鍵コード１」とは異なる「鍵コード２」を生成し、ステップＧ１８１５において「鍵コード２」により鍵ボックス部２１４から鍵を選択し「鍵ＫＣ２」とし、ステップＧ１８１６においてＤ１を「鍵ＫＣ２」を鍵として暗号部２１０で暗号化：Ｅ２＝（ＫＣ２、Ｄ１）してＥ２を作成し、ステップＧ１８１７において、Ｅ２と「鍵コード２」を半導体チップ１０１ｄに送信し、ステップＧ１８１８においてＤ１と「鍵ＫＣ１」と「鍵ＫＣ２」を排他的論理和ＫＩ１＝Ｄ１＾ＫＣ１＾ＫＣ２（＾は排他的論理和をあらわす記号とする）して記録、または再生に必要なデータを暗号化伝送するための鍵として用いる伝送鍵である「ＫＩ１」を作成する。

【００８６】

ステップＧ４の処理である図４２では、ステップＧ１８２１において、Ｅ２と「鍵コード２」を受信し、ＣＰＵ１１１ｄはステップＧ１８２２において、鍵ボックス部１２１で「鍵コード２」に対応した「鍵ＫＣ２」を選択し、ステップＧ１８２３においてＥ２を「鍵ＫＣ２」を鍵として暗号部１２０で復号化：Ｄ２＝（ＫＣ２、Ｅ２）を実行してＤ２を作成し、ステップＧ１８２４において、乱数

ＲＸとＤ２を比較して、乱数ＲＸとＥ２が不一致の場合（ｎｏ）には、ステップＧ１８２７に進んで通信終了を送信し、ステップＧ１８２８において通信終了する。

【００８７】

一方、上記ステップＧ１８２４において乱数ＲＸとＥ２が一致した場合（ｙｅｓ）には、半導体チップ１０１ｄは記録再生装置４００を認証し、ステップＧ１８２５においてＲＸと「鍵ＫＣ１」と「鍵ＫＣ２」を排他的論理和Ｋ１２＝ＲＸ＾ＫＣ１＾ＫＣ２して記録、または再生に必要なデータを暗号化伝送するための鍵として用いる伝送鍵である「ＫＩ２」を作成し、ステップＧ１８２５において継続コマンドを送信する。

【００８８】

ステップＧ１の処理である図４３では、ステップＧ１５３１において、継続コマンド、または通信終了を受信し、ステップＧ１５３２において、上記受信した情報が継続コマンドか否かを確認し、これが継続コマンドではないと判定された場合（ｎｏ）には、ステップＧ１５３４に進んで通信終了し、逆に、継続コマンドであると判定された場合（ｙｅｓ）には、ステップＧ１５０３に進んで再生動作を行う。

【００８９】

このように本実施の形態５によれば、ディスクメディア１００の半導体チップ１０１ｄに暗号処理機能を設け、暗号を用いて認証を行うようにしたので、暗号通信可能なこ環境下でのみディスクメディアの再生が許可されることとなり、より、コンテンツのセキュリティを高めることができる。

さらに、ステップＧ１８１８およびステップ１８２５において、乱数データを含む通信過程のデータを用いて、記録または再生動作で必要なデータを暗号化して伝送するための伝送鍵を認証ごとに異ように生成するので、安全性の高い鍵を作成できる。

【００９０】

なお、上記実施の形態１では、ディスクメディア１００に搭載される半導体チップ１０１に電源や信号を供給するのに、クリッピング領域１０３にワイヤー配

線１０５を用いて行う例を示したが、例えば、クリッピング領域に太陽電池パネルを搭載し、これによって半導体チップに電源を供給するとともに、半導体レーザを太陽電池パネルの特定位置に照射することで、信号のやり取りを行うような構成とすることも可能である。

【００９１】

また、上記実施の形態３では、ディスクメディアに個人情報としてパスワードを保持さ、これを確認させたり、実施の形態５では、暗号処理を用いてディスクメディアと再生装置との間での認証を行うようにしたが、認証にかかるアルゴリズムをＩＣカードなどの媒体に持たせ、ＩＣカードなどの媒体をコンテンツ再生時に鍵代わりに用いるようにすることで、不正利用を防止するようにすることも可能である。

【００９２】

さらに、上記各実施の形態では、コンテンツを記録する媒体として、ディスクメディアを例にとって説明したが、他にも、ＨＤＤやテープや、ＲＯＭなどについても、これらに記録されたコンテンツの再生を管理する半導体チップを具備することで、上記各実施の形態と同様の効果を得ることができる。

【００９３】

【発明の効果】

以上のように、この発明の請求項１にかかるデータ記憶媒体によれば、コンテンツ記録用または再生用のデータ記録媒体において、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行う自立型再生履歴管理機能付き回路を具備したものとしたので、コンテンツの再生を自己で管理することができ、コピー元の記録媒体を用いた無制限な複製を防止することができ、著作権の侵害を効果的に防止することができるという効果が得られる。

【００９４】

また、この発明の請求項２にかかるデータ記憶媒体によれば、上記請求項１記載のデータ記録媒体において、上記コンテンツは鍵を用いて暗号化されて上記ディスクメディアに記録され、上記自立型再生履歴管理機能付き回路は、上記ディ

スクメディアに記録されたコンテンツを復号化するための復号鍵を記憶するとともに、上記ディスクメディアからコンテンツが再生される際に復号化されたコンテンツのディジタル形式での出力回数を制限するコンテンツ出力管理部とを有するものとしたので、や、物理的なスタンプコピーなどを行ってもコンテンツが暗号化されているために、再生することができず、著作権の侵害を効果的に防止することができるという効果が得られる。

【００９５】

また、この発明の請求項３にかかるデータ記憶媒体によれば、上記請求項２記載のデータ記録媒体において、上記ディスクメディアに記録されたコンテンツは、タイトル単位または任意のデータサイズ単位で異なる鍵を用いて暗号化され、上記コンテンツ出力管理部は、上記コンテンツの暗号化単位ごとの復号鍵を有し、コンテンツのタイトル単位または任意のデータサイズ単位でのディジタル形式での出力回数を制限するようにしたので、コンテンツの著作権をより強固なものとすることができるという効果が得られる。

【００９６】

また、この発明の請求項４にかかるデータ記憶媒体によれば、上記請求項２記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で出力される際に、その回数を更新記録し、該回数を予め設定された制限回数と比較し、コンテンツのディジタル形式での出力回数が上記制限回数を超えた場合には上記コンテンツのディジタル形式での出力を抑制するようにしたので、コンテンツのディジタル形式での複製回数を制限することができるという効果が得られる。

【００９７】

また、この発明の請求項５にかかるデータ記憶媒体によれば、上記請求項４記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記コンテンツがディジタル形式で同時に複数の経路で出力される際に、その経路の数を記録する出力経路数記憶部を有し、コンテンツのディジタル形式での出力回数の計数時に上記出力経路数記憶部に記憶された経路の数を加味してコンテンツのディジタル形式での出力を計数するようにしたので、ディジタル形式の出力インターフェイ

スを複数個備えた再生装置においても、複製回数を管理することができるという効果がある。

【００９８】

また、この発明の請求項６にかかるデータ記憶媒体によれば、上記請求項１記載のデータ記録媒体において、上記コンテンツ出力管理部は、上記ディスクメディアの所有者を認識するための個人情報を記憶する個人情報記憶部を有し、上記コンテンツ再生時に外部より入力された情報と上記個人情報とを比較し、比較結果が一致した場合にのみ上記コンテンツの再生を許可するようにしたので、データ記憶媒体の所有者以外の不特定な人物がコンテンツを無許可で再生することを防止することができるという効果が得られる。

【００９９】

また、この発明の請求項７にかかるデータ記憶媒体は、請求項６記載のデータ記録媒体において、上記コンテンツ出力管理部は、外部より入力された情報と上記個人情報とを比較し、比較結果が連続して不一致になった場合に、該不一致回数を記憶する不一致回数保持部を備え、不一致回数が所定値よりも大きくなった場合には上記コンテンツの再生を抑制するとともに、外部に通知するものである。

【０１００】

また、この発明の請求項８にかかるデータ管理システムは、上記コンテンツ記録用または再生用のデータ記録媒体を用いてデータを管理するデータ管理システムにおいて、上記データ記録媒体に、著作権保護情報を記録し、コンテンツ再生時に該情報を参照してコンテンツの再生出力の管理を行うとともに、コンテンツ出力時に該コンテンツを所定のアルゴリズムに従って暗号化処理する自立型再生履歴管理機能付き回路を具備し、記録再生装置に、上記自立型再生履歴管理機能付き回路と同一のアルゴリズムにて暗号化処理を行うメディア管理部を備え、上記コンテンツ再生時に、暗号化されたコンテンツを復号化して再生するようにしたので、コンテンツの著作権を効果的に保護することができるという効果が得られる。

【０１０１】

また、この発明の請求項９にかかるデータ管理システムは、上記請求項８記載のデータ管理システムにおいて、上記コンテンツ再生時に、上記データ記録媒体の自立型再生履歴管理機能付き回路による暗号化処置と、上記メディア管理部の暗号化処理とを用いて、データ記録媒体と上記記録再生装置との間での認証を行い、該認証結果によって上記コンテンツの復号化の可否を判定するようにしたので、データ記録媒体と記録再生装置との間で認証を行うことができ、コンテンツの著作権の保護をさらに強固なものとすることができるという効果が得られる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１によるデータ記憶媒体であるディスクメディアの概念的な構成を示す図である。

【図２】　上記実施の形態１のディスクメディアのワイヤー配線を含む構成を示す図である。

【図３】　上記実施の形態１のディスクメディアに記録されたコンテンツを再生もしくは、コンテンツを記録する際に使用する記録再生装置と上記ディスクメディアの配置を示す図（ａ）、及びディスクメディアを回転させるためのモータに載置した状態を示す図（ｂ）である。

【図４】　上記実施の形態１の半導体チップの構成を模式的に示す構成図である。

【図５】　上記実施の形態１によるデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【図６】　上記実施の形態１によるデータ管理システムを用いてコンテンツを暗号化して記録する際の全体的な動作を示す図である。

【図７】　上記実施の形態１によるデータ管理システムの記録時のステップＺ１の詳細な工程を示す図である。

【図８】　上記実施の形態１によるデータ管理システムのステップＺ２の記録時の詳細な工程を示す図である。

【図９】　上記実施の形態１によるデータ管理システムのステップＺ３の記録時の詳細な工程を示す図である。

【図１０】　本発明実施の形態１によるディスクメディアに記録されたコン

テンツを記録再生装置によって再生する際の全体的な動作を説明するための図である。

【図１１】　上記実施の形態１によるデータ管理システムのコンテンツを再生する際のステップＡ１の詳細な工程を示す図である。

【図１２】　上記実施の形態１によるデータ管理システムのコンテンツを再生する際のステップA２の詳細な工程を示す図である。

【図１３】　上記実施の形態１によるデータ管理システムのコンテンツを再生する際のステップA３の詳細な工程を示す図である。

【図１４】　上記実施の形態１によるデータ管理システムのコンテンツを再生する際のステップA４の詳細な工程を示す図である。

【図１５】　本発明の実施の形態２によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図１６】　上記実施の形態２によるデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【図１７】　本発明実施の形態２によるディスクメディアに記録されたコンテンツを記録再生装置によって再生する際の全体的な動作を説明するための図である。

【図１８】　上記実施の形態２によるデータ管理システムのコンテンツを再生する際のステップＢ１の詳細な工程を示す図である。

【図１９】　上記実施の形態２によるデータ管理システムのコンテンツを再生する際のステップＢ２の詳細な工程を示す図である。

【図２０】　上記実施の形態２によるデータ管理システムのコンテンツを再生する際のステップＢ３の詳細な工程を示す図である。

【図２１】　上記実施の形態２によるデータ管理システムのコンテンツを再生する際のステップＢ４の詳細な工程を示す図である。

【図２２】　本発明の実施の形態３によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図２３】　上記実施の形態３によるデータ記憶媒体を用いたデータ管理システムの個人情報を登録する手順を示す全体的な構成図である。

【図２４】　上記実施の形態３によるデータ管理システムの個人情報を登録する手順であるステップＣ１の詳細な工程を示す図である。

【図２５】　上記実施の形態３によるデータ管理システムの個人情報を登録する手順であるステップＣ２の詳細な工程を示す図である。

【図２６】　上記実施の形態３によるデータ管理システムの個人情報を登録する手順であるステップＣ３の詳細な工程を示す図である。

【図２７】　上記実施の形態３によるデータ管理システムの個人情報を登録する手順であるステップＣ４の詳細な工程を示す図である。

【図２８】　上記実施の形態３によるデータ記憶媒体を用いたデータ管理システムの登録された個人情報を確認するための手順を示す全体的な構成図である。

【図２９】　上記実施の形態３によるデータ管理システムの登録された個人情報を確認するための手順であるステップＤ３の詳細な工程を示す図である。

【図３０】　上記実施の形態３によるデータ管理システムの登録された個人情報を確認するための手順であるステップＤ４の詳細な工程を示す図である。

【図３１】　上記実施の形態３によるデータ管理システムの登録された個人情報を確認するための手順であるステップＤ５の詳細な工程を示す図である。

【図３２】　本発明の実施の形態４によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図３３】　上記実施の形態４によるデータ記憶媒体を用いたデータ管理システムの個人情報確認時の不正アクセスを記録するための手順を示す全体的な構成図である。

【図３４】　上記実施の形態４によるデータ管理システムの不正アクセスを記録する手順であるステップＥ４の詳細な工程を示す図である。

【図３５】　上記実施の形態４によるデータ管理システムの不正アクセスを記録する手順であるステップＥ５の詳細な工程を示す図である。

【図３６】　本発明の実施の形態５によるデータ記憶媒体であるディスクメディアに搭載された半導体チップの構成を模式的に示す構成図である。

【図３７】　上記実施の形態５によるデータ記憶媒体を用いたデータ管理シ

ステムの全体的な構成を示す構成図である。

【図３８】　上記実施の形態５によるデータ管理システムのコンテンツを再生する際の暗号アルゴリズムによる認証を行う際の全体的な動作を説明するための図である。

【図３９】　上記実施の形態５によるデータ管理システムの認証を行う手順であるステップＧ１の詳細な工程を示す図である。

【図４０】　上記実施の形態５によるデータ管理システムの認証を行う手順であるステップＧ２の詳細な工程を示す図である。

【図４１】　上記実施の形態５によるデータ管理システムの認証を行う手順であるステップＧ３の詳細な工程を示す図である。

【図４２】　上記実施の形態５によるデータ管理システムの認証を行う手順であるステップＧ４の詳細な工程を示す図である。

【図４３】　上記実施の形態５によるデータ管理システムの認証を行う手順であるステップＧ５の詳細な工程を示す図である。

【図４４】　従来のデータ管理システムによる著作権保護方式の一例である、ＣＧＭＳ(Copy Generation Management System)方式を説明するための図である。

【図４５】　従来のデータ記憶媒体を用いたデータ管理システムの全体的な構成を示す構成図である。

【符号の説明】

９０　　センタホール

１００　ディスクメディア

１０１ａ～１０１ｄ　半導体チップ

１０２　データ領域

１０３　クリッピング領域

１０４　ＴＯＢ（Table of contents）領域

１０５　ワイヤー配線

１０６　トレイ

１０７　クリッピング

１０８　ワイヤー配線

１０９　スピンドルモータ

１１０　Ｉ／Ｏ

１１１　ＣＰＵ

１１２　記憶部

１１４　タイトル

１１５　復号鍵部

１１６　ディジタル出力制限回数情報

１１７　個人情報保持部

１１８　不正回数保持部

１１９　暗号部

１２０　乱数部

１２１　記憶部

２００，３００，４００　記録再生装置

２０１　暗号部

２０２　メディア管理部

２０３　ＣＰＵ

２０４　ディジタルインターフェイス

２０５　Ｄ／Ａ変換器

２０６　ユーザ設定部

２０７　表示部

２０８　光ピックアップ

２０９　Ａ／Ｄ変換器

２１０　暗号部

２１１　乱数部

２１２　外部記録再生装置

２１３　接続ケーブル

２１４　鍵ボックス部

３０１　ディジタルインターフェイス（Ａ）

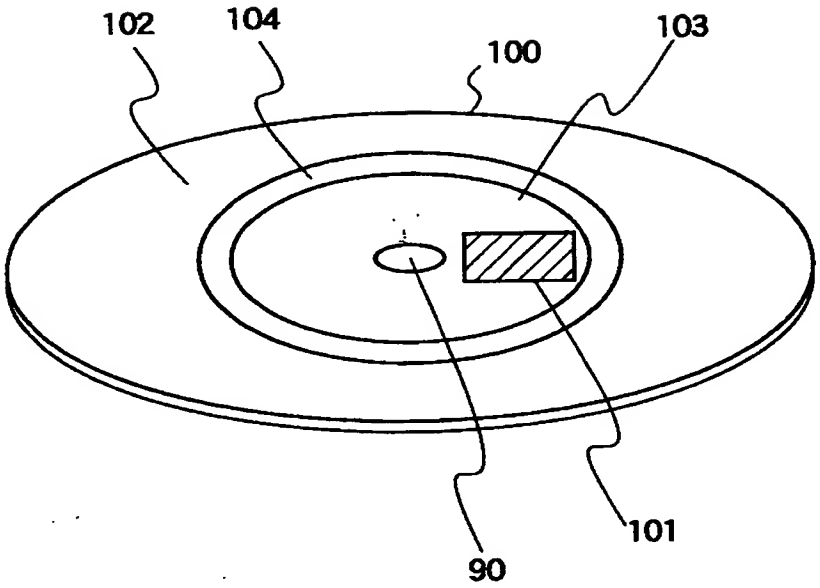
３０２　ディジタルインターフェイス（Ｂ）

３０３　ＨＤＤ装置（Ａ）

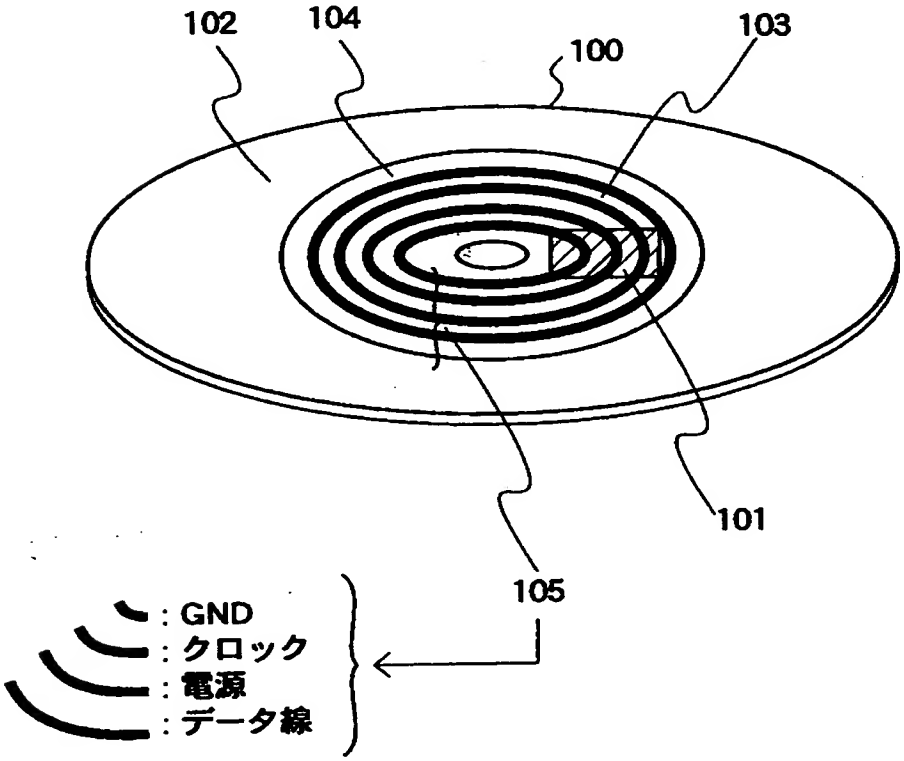
３０４　ＨＤＤ装置（Ｂ）

【書類名】　図面

【図１】

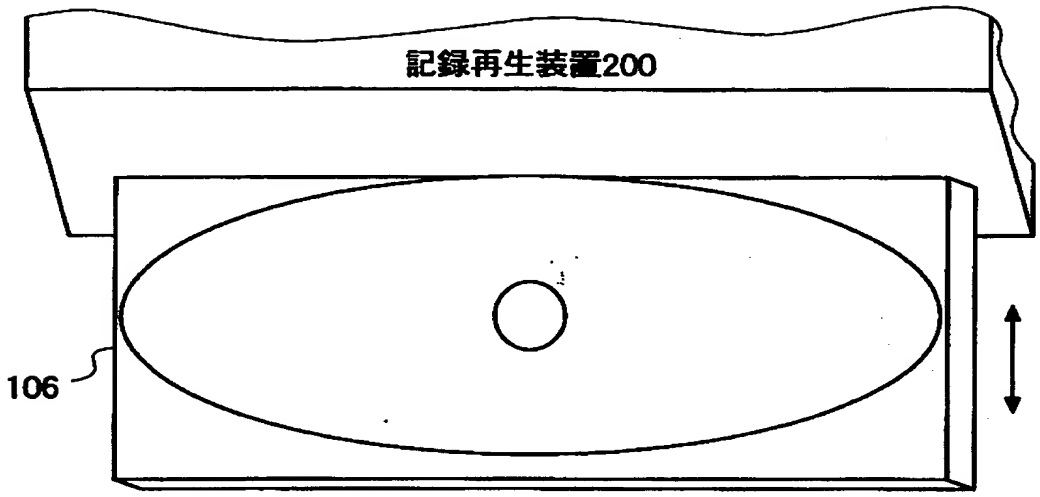



【図２】

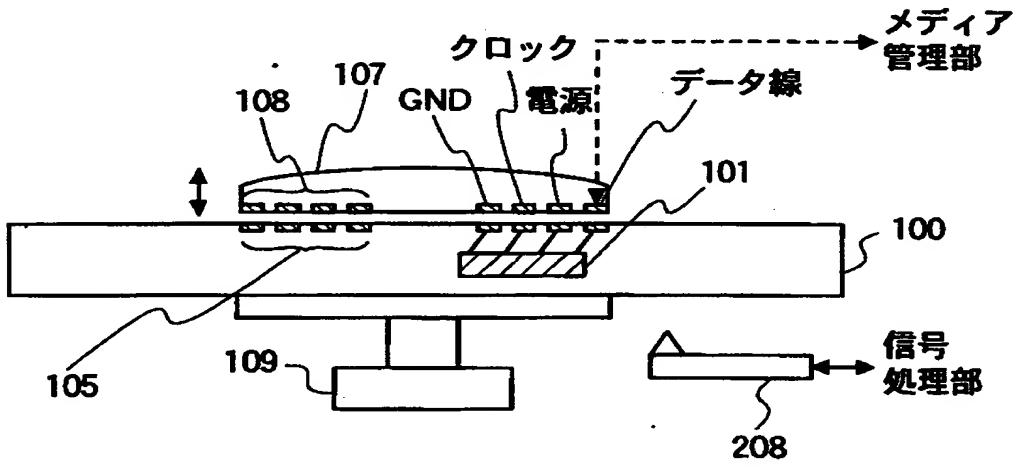


【図３】

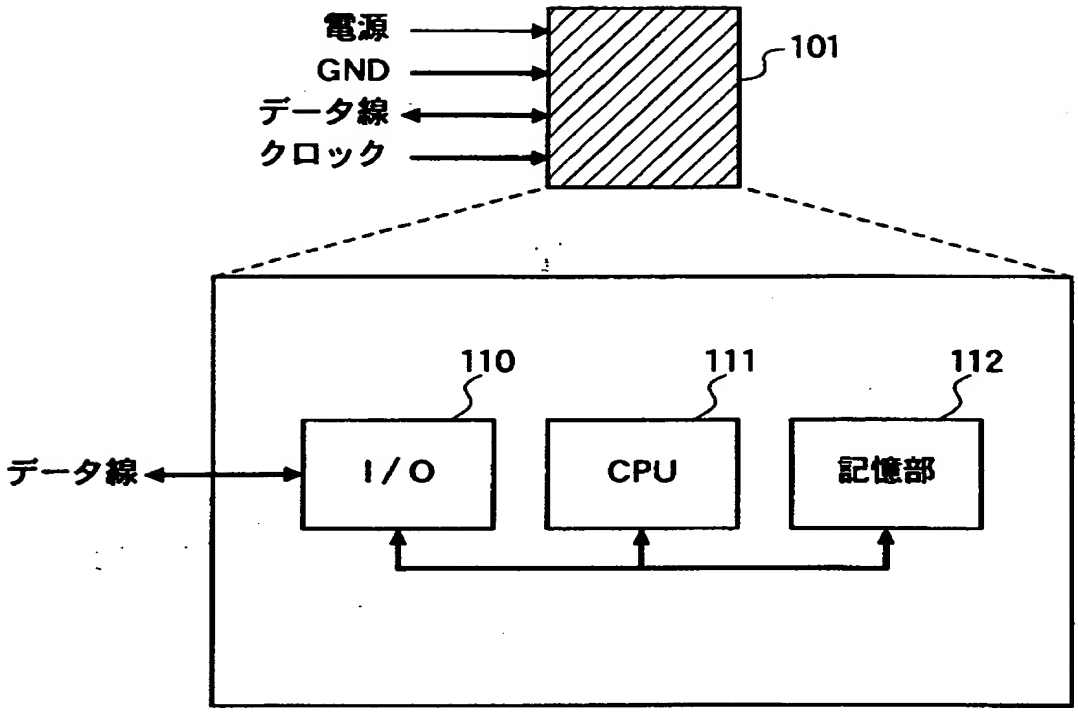
(a)


記録再生装置200
106

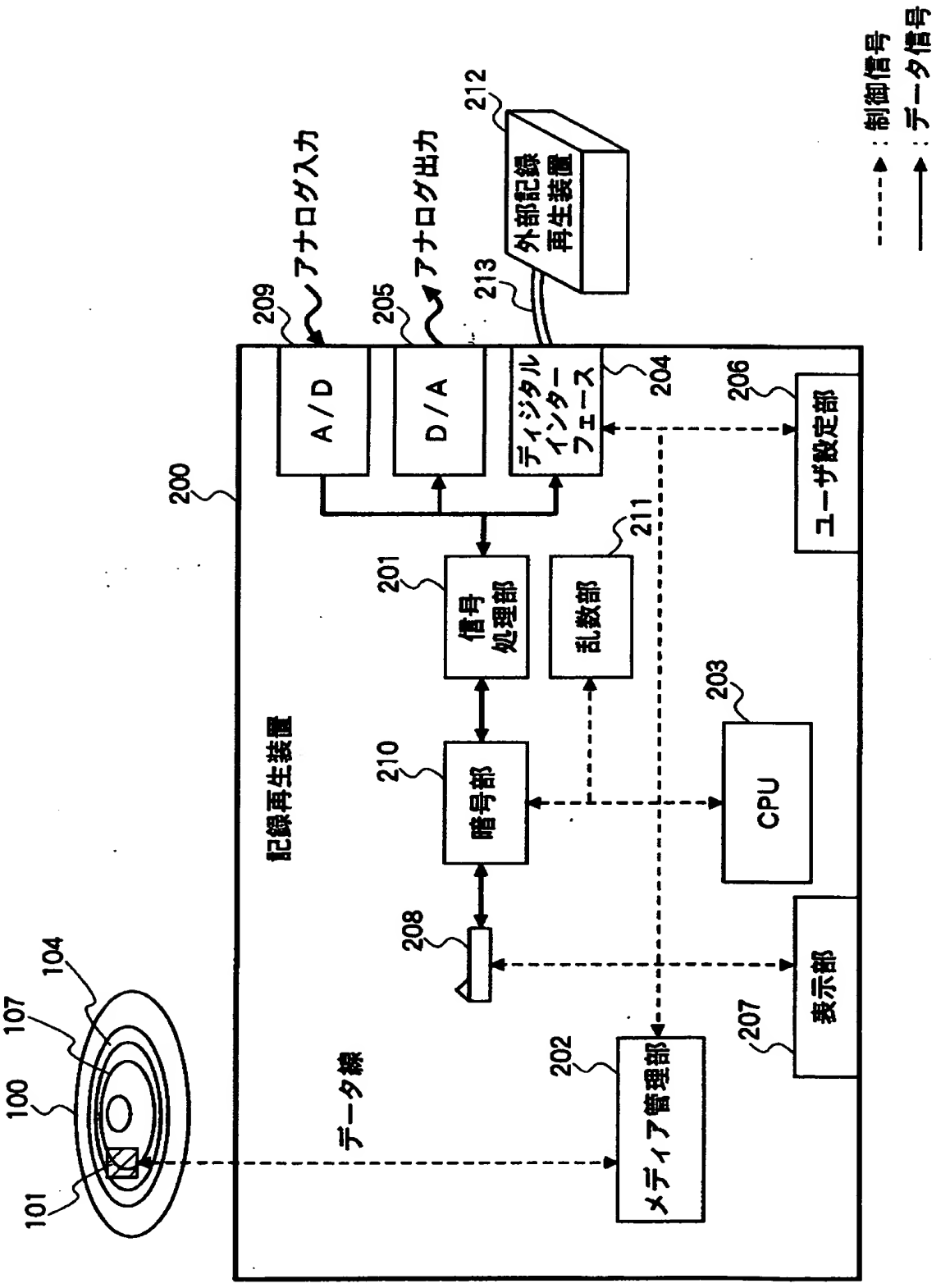
(b)


メディア
管理部
クロック
107
108
GND
電源
データ線
101
100
105
109
信号
処理部
208

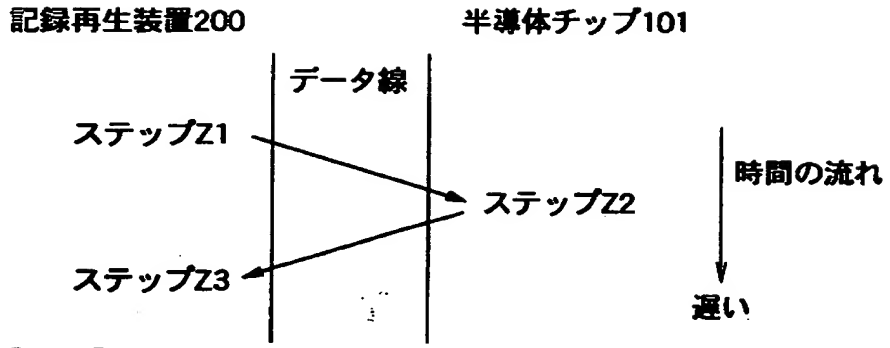
【図４】



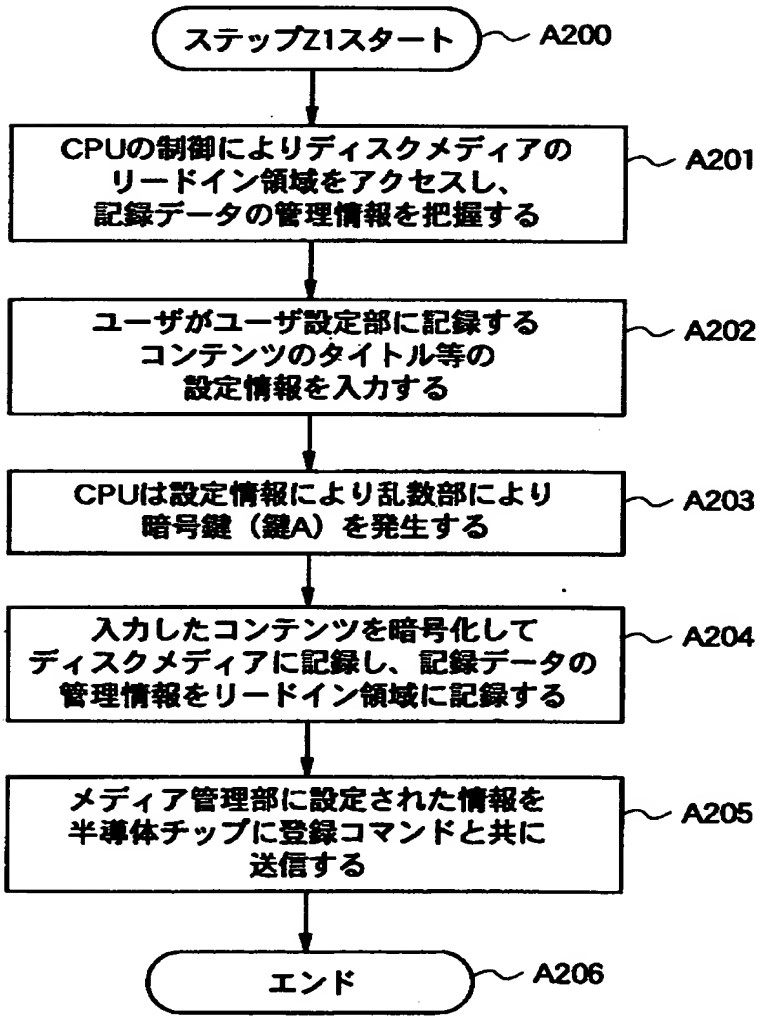
【図５】


：制御信号
：データ信号
212
外部記録再生装置
213
209
アナログ入力
205
アナログ出力
A/D
D/A
ディジタルインターフェース
204
206
ユーザ設定部
200
201
信号処理部
211
乱数部
記録再生装置
210
暗号部
203
CPU
208
207
表示部
104
107
100
101
データ線
202
メディア管理部

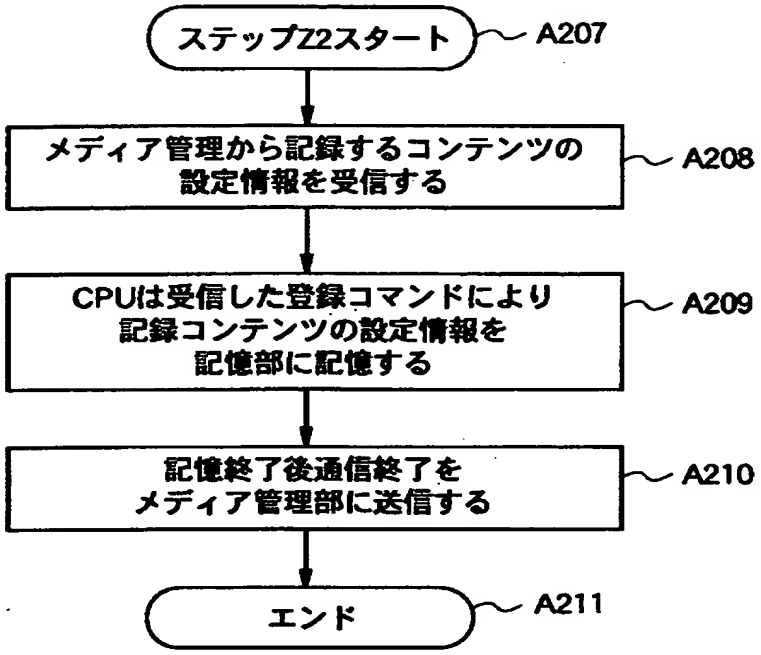
【図６】


記録再生装置200
半導体チップ101
データ線
ステップZ1
ステップZ2
ステップZ3
時間の流れ
遅い

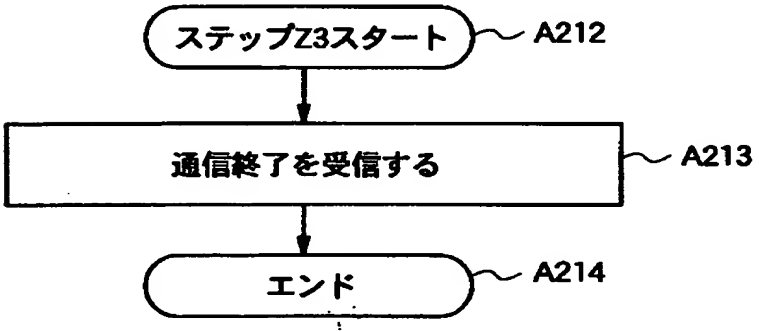
【図７】


ステップZ1スタート
A200
CPUの制御によりディスクメディアの
リードイン領域をアクセスし、
記録データの管理情報を把握する
A201
ユーザがユーザ設定部に記録する
コンテンツのタイトル等の
設定情報を入力する
A202
CPUは設定情報により乱数部により
暗号鍵（鍵A）を発生する
A203
入力したコンテンツを暗号化して
ディスクメディアに記録し、記録データの
管理情報をリードイン領域に記録する
A204
メディア管理部に設定された情報を
半導体チップに登録コマンドと共に
送信する
A205
エンド
A206

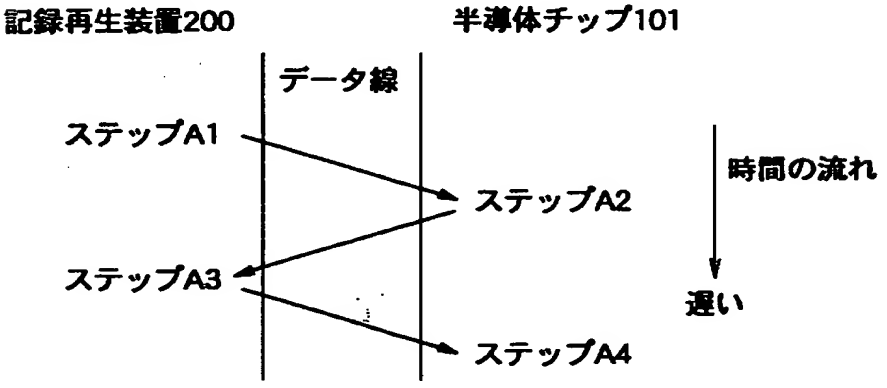
【図８】


ステップZ2スタート
A207
メディア管理から記録するコンテンツの設定情報を受信する
A208
CPUは受信した登録コマンドにより記録コンテンツの設定情報を記憶部に記憶する
A209
記憶終了後通信終了をメディア管理部に送信する
A210
エンド
A211

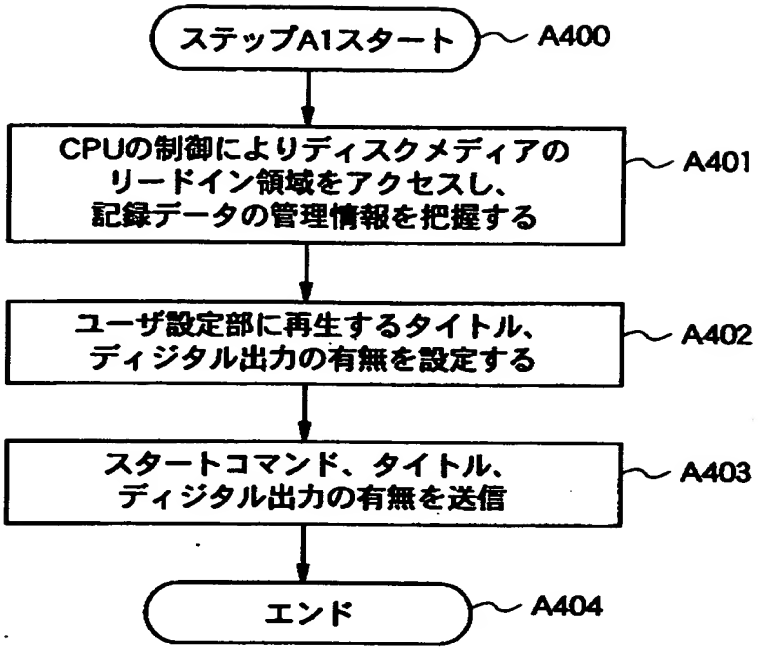
【図９】


ステップZ3スタート
A212
通信終了を受信する
A213
エンド
A214

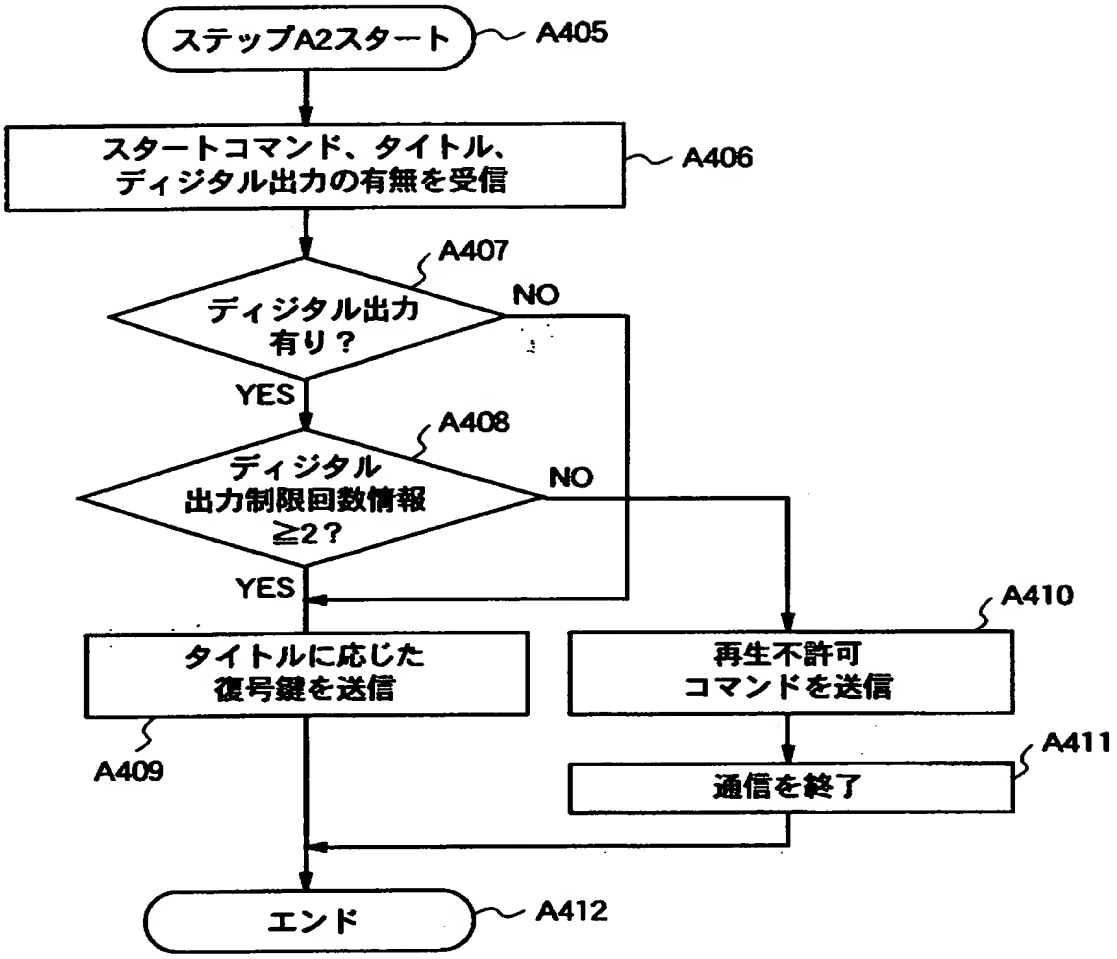
【図１０】


記録再生装置200
半導体チップ101
データ線
ステップA1
ステップA2
ステップA3
ステップA4
時間の流れ
遅い

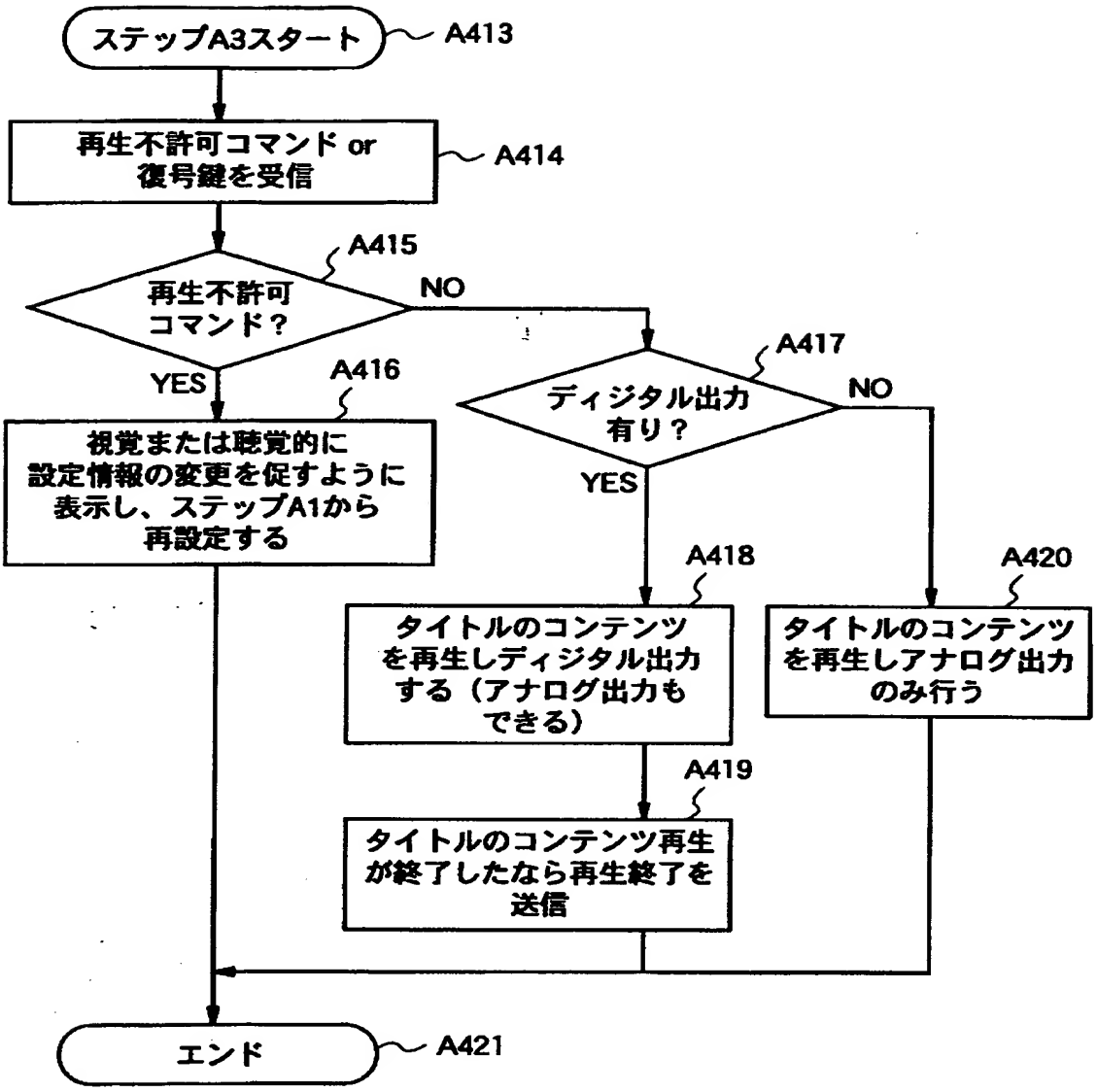
【図１１】


ステップA1スタート
A400
CPUの制御によりディスクメディアの
リードイン領域をアクセスし、
記録データの管理情報を把握する
A401
ユーザ設定部に再生するタイトル、
ディジタル出力の有無を設定する
A402
スタートコマンド、タイトル、
ディジタル出力の有無を送信
A403
エンド
A404

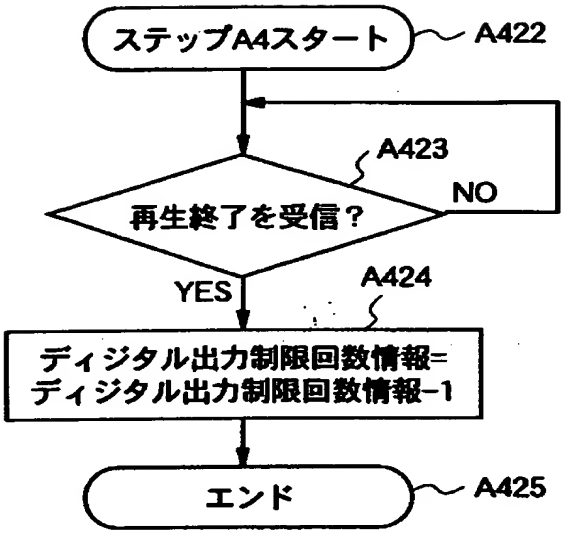
【図１２】


ステップA2スタート
A405
スタートコマンド、タイトル、
ディジタル出力の有無を受信
A406
A407
ディジタル出力
有り？
NO
YES
A408
ディジタル
出力制限回数情報
≧2？
NO
YES
A410
タイトルに応じた
復号鍵を送信
再生不許可
コマンドを送信
A409
A411
通信を終了
エンド
A412

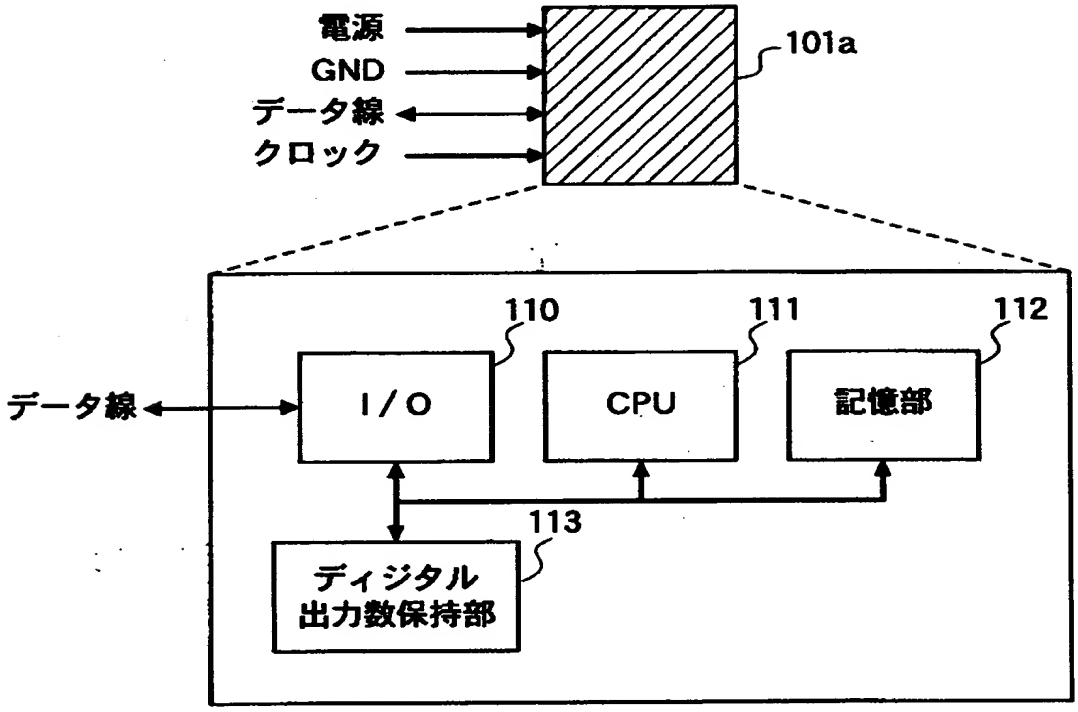
【図１３】


ステップA3スタート
A413
再生不許可コマンド or 復号鍵を受信
A414
A415
再生不許可コマンド？
NO
YES
A416
視覚または聴覚的に設定情報の変更を促すように表示し、ステップA1から再設定する
A417
ディジタル出力有り？
NO
YES
A418
タイトルのコンテンツを再生しディジタル出力する（アナログ出力もできる）
A419
タイトルのコンテンツ再生が終了したなら再生終了を送信
A420
タイトルのコンテンツを再生しアナログ出力のみ行う
エンド
A421

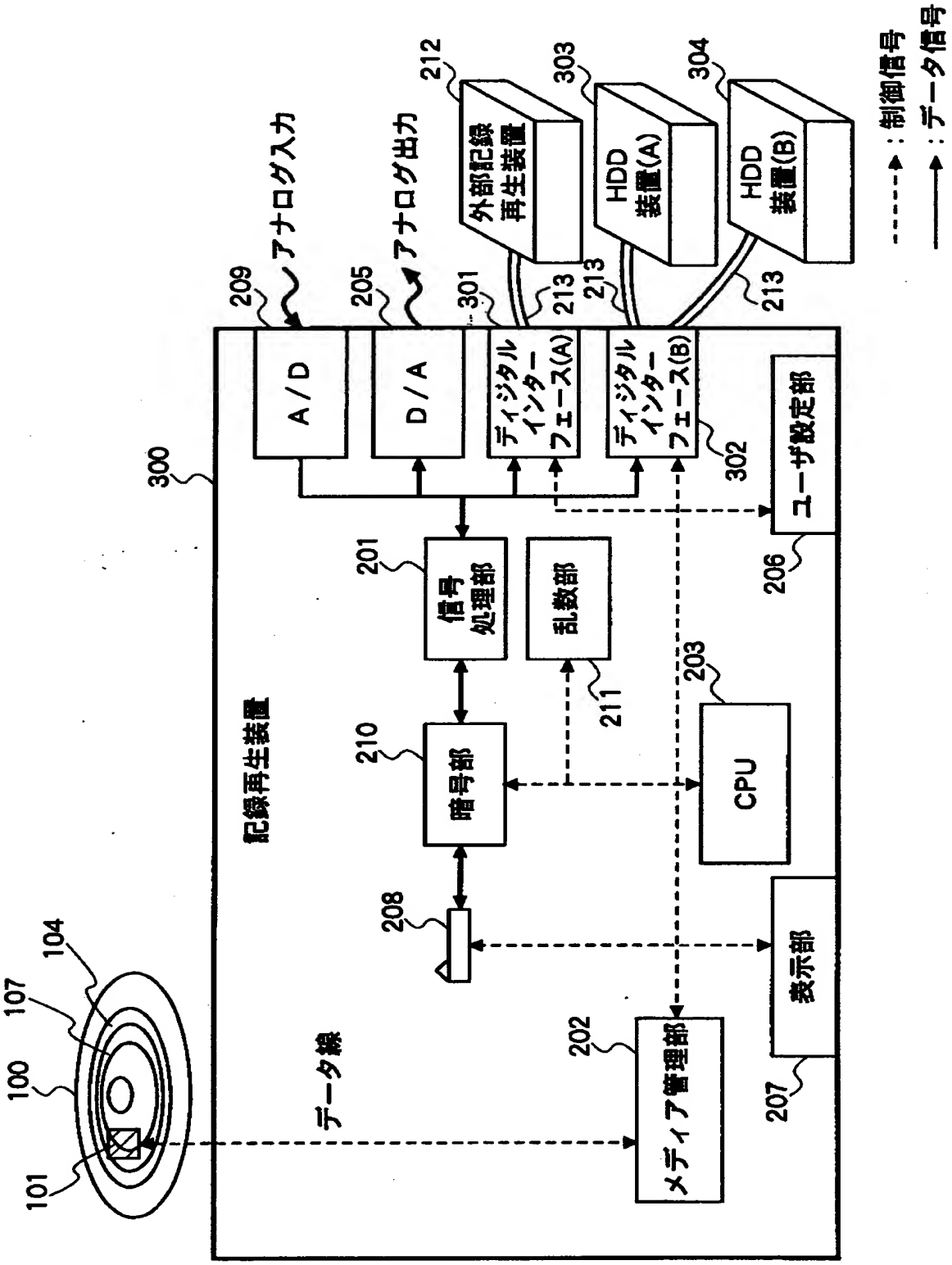
【図１４】


ステップA4スタート
A422
A423
再生終了を受信？
NO
YES
A424
ディジタル出力制限回数情報=
ディジタル出力制限回数情報−1
エンド
A425

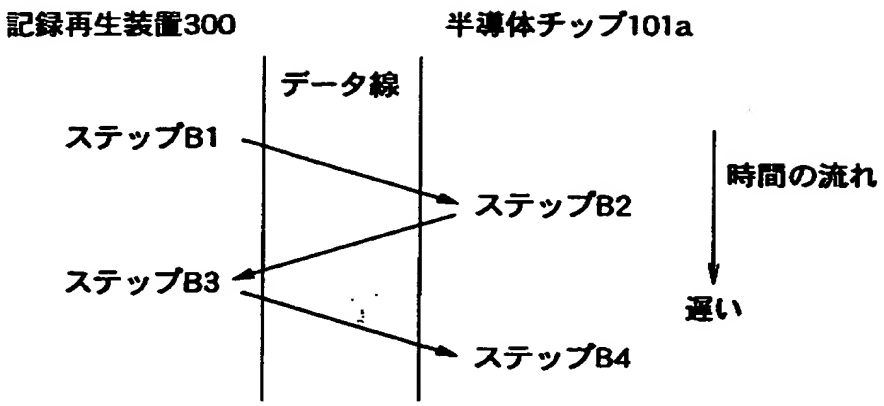
【図１５】


電源
GND
データ線
クロック
101a
110
111
112
データ線
I/O
CPU
記憶部
113
ディジタル
出力数保持部

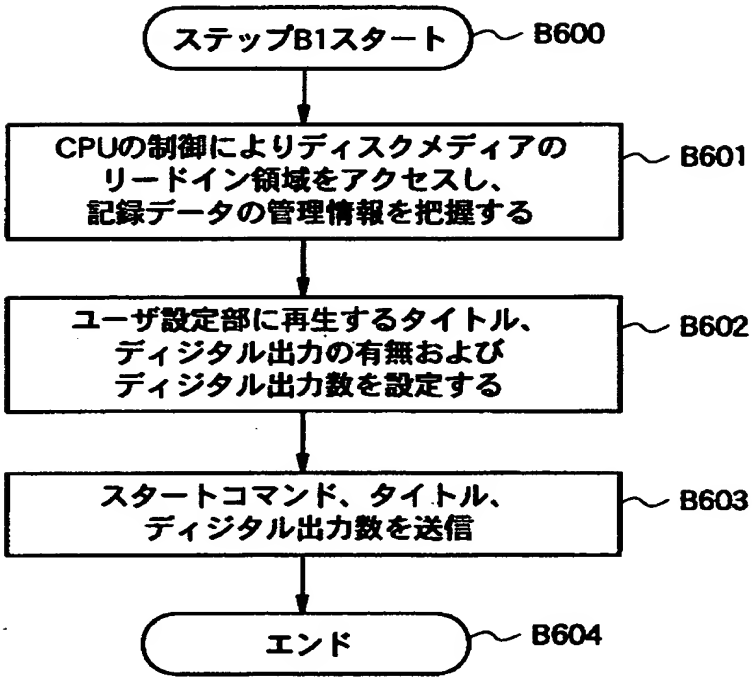
【図１６】


：制御信号
：データ信号
記録再生装置
300
A/D
D/A
ディジタル インター フェース(A)
ディジタル インター フェース(B)
ユーザ設定部
信号 処理部
乱数部
暗号部
CPU
表示部
メディア管理部
外部記録 再生装置
HDD 装置(A)
HDD 装置(B)
アナログ入力
アナログ出力
データ線
209
205
301
213
212
303
304
302
206
201
211
203
210
208
207
202
104
107
100
101

【図１７】



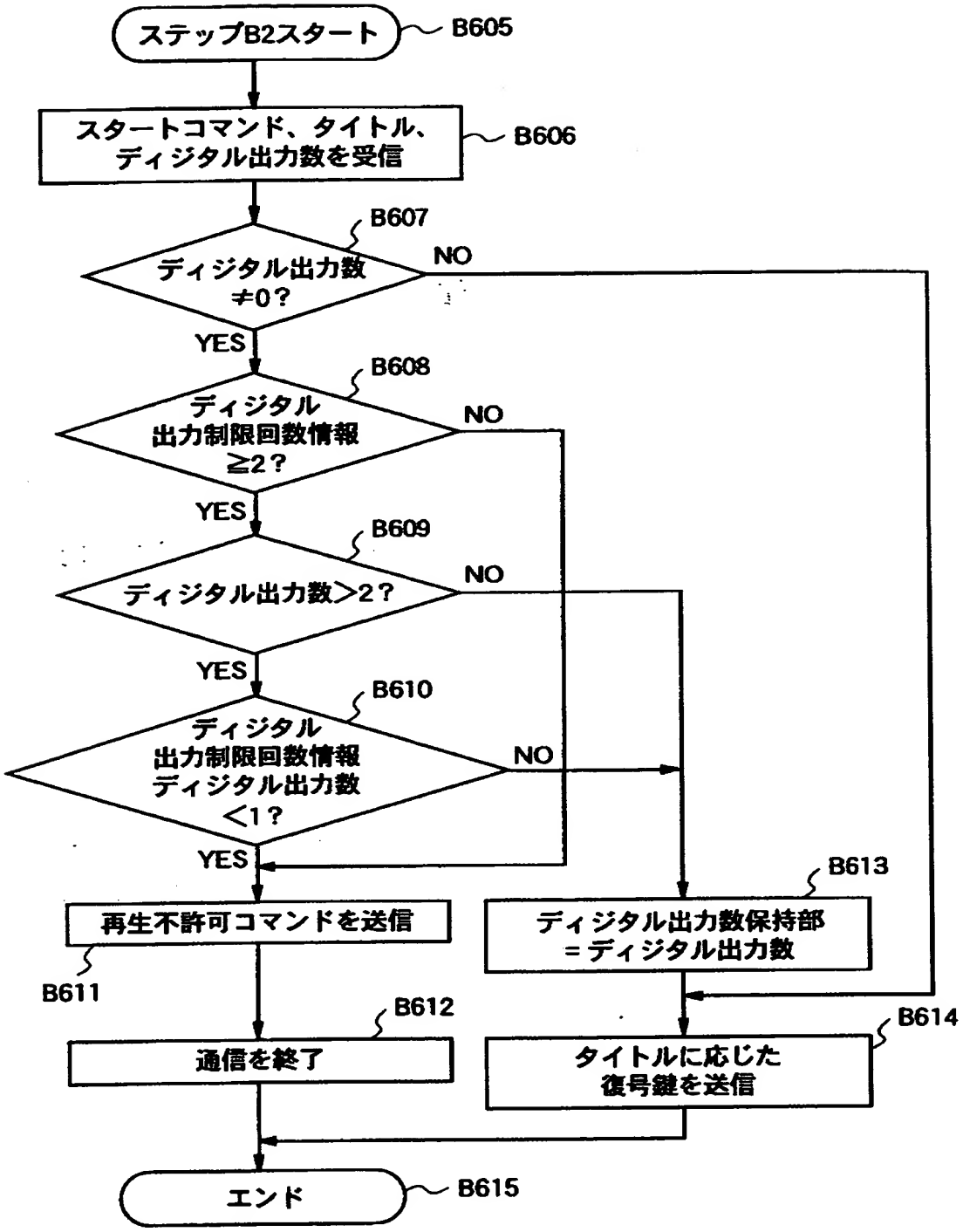

【図１８】



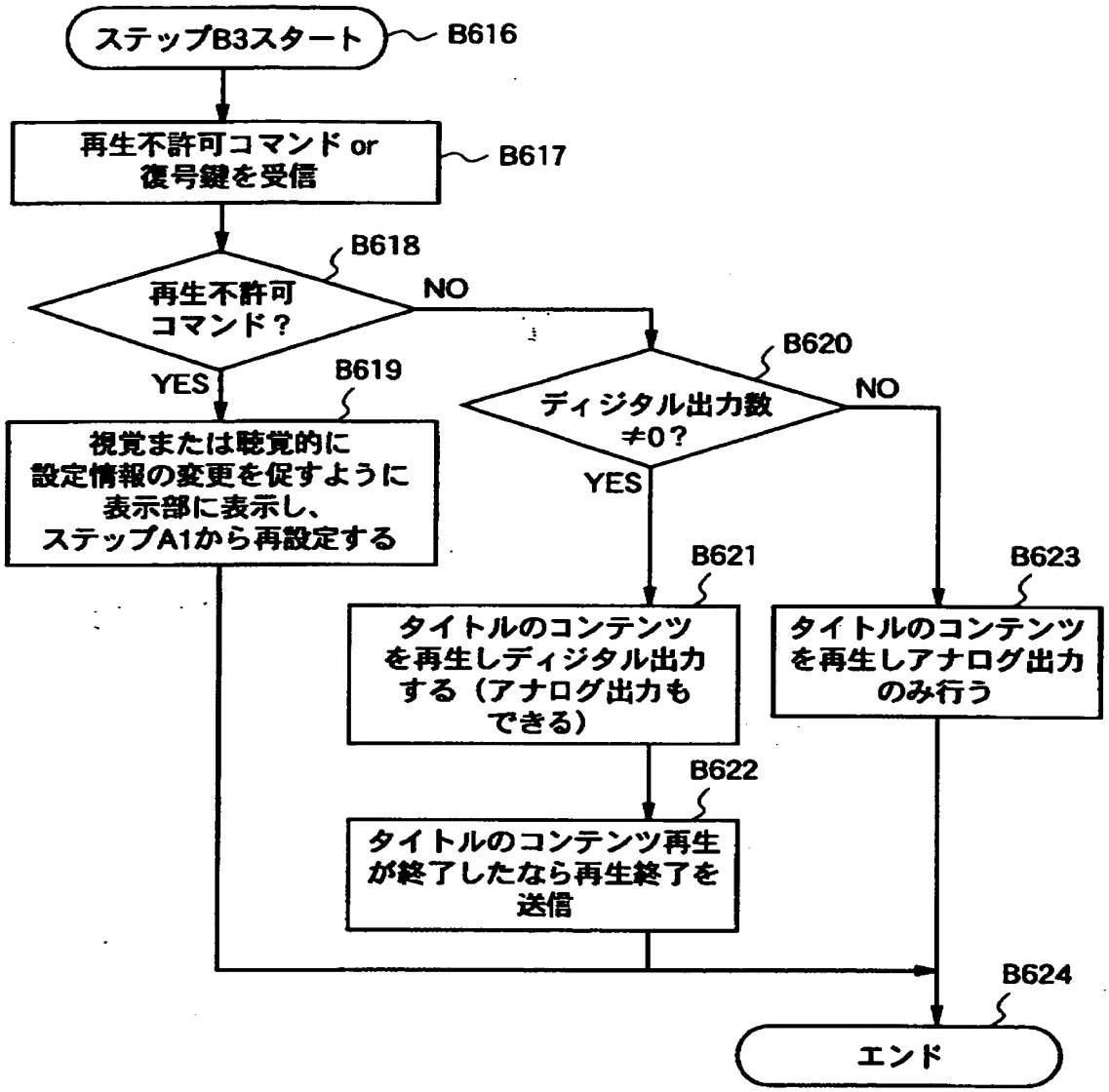


出証特２０００－３０６４３８１

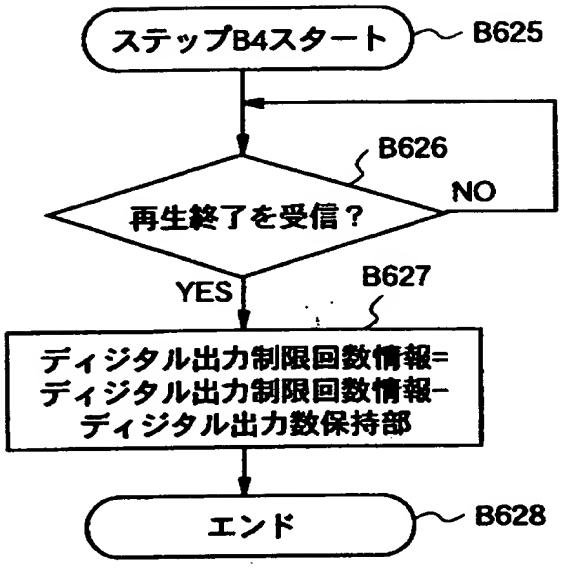
【図１９】


ステップB2スタート
B605
スタートコマンド、タイトル、ディジタル出力数を受信
B606
B607
ディジタル出力数≠0?
NO
YES
B608
ディジタル出力制限回数情報≧2?
NO
YES
B609
ディジタル出力数>2?
NO
YES
B610
ディジタル出力制限回数情報ディジタル出力数<1?
NO
YES
B613
再生不許可コマンドを送信
ディジタル出力数保持部=ディジタル出力数
B611
B612
B614
通信を終了
タイトルに応じた復号鍵を送信
エンド
B615

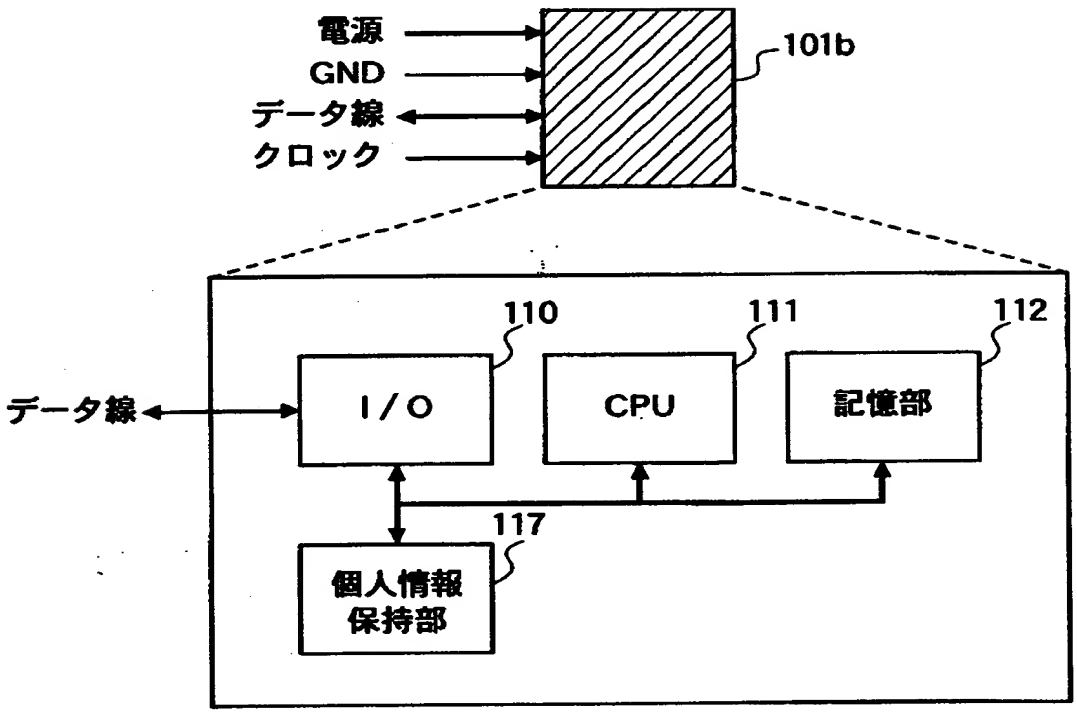
【図２０】


ステップB3スタート
B616
再生不許可コマンドor
復号鍵を受信
B617
B618
再生不許可
コマンド？
NO
YES
B619
視覚または聴覚的に
設定情報の変更を促すように
表示部に表示し、
ステップA1から再設定する
B620
ディジタル出力数
≠0？
NO
YES
B621
タイトルのコンテンツ
を再生しディジタル出力
する（アナログ出力も
できる）
B622
タイトルのコンテンツ再生
が終了したなら再生終了を
送信
B623
タイトルのコンテンツ
を再生しアナログ出力
のみ行う
B624
エンド

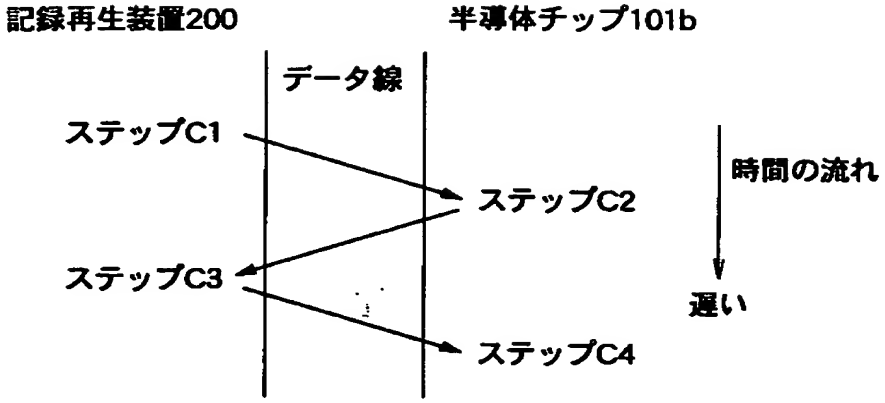
【図２１】


ステップB4スタート
B625
B626
再生終了を受信？
NO
YES
B627
ディジタル出力制限回数情報=
ディジタル出力制限回数情報−
ディジタル出力数保持部
エンド
B628

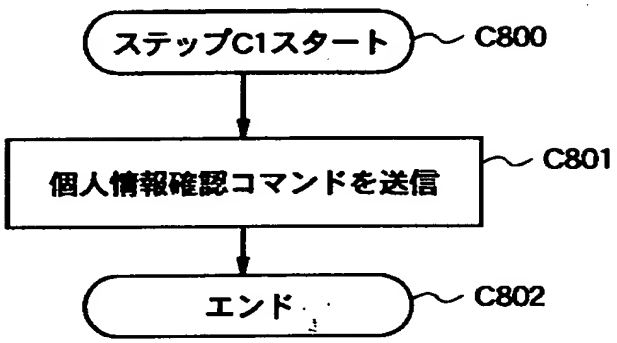
【図２２】


電源
GND
データ線
クロック
101b
110
111
112
データ線
I/O
CPU
記憶部
117
個人情報
保持部

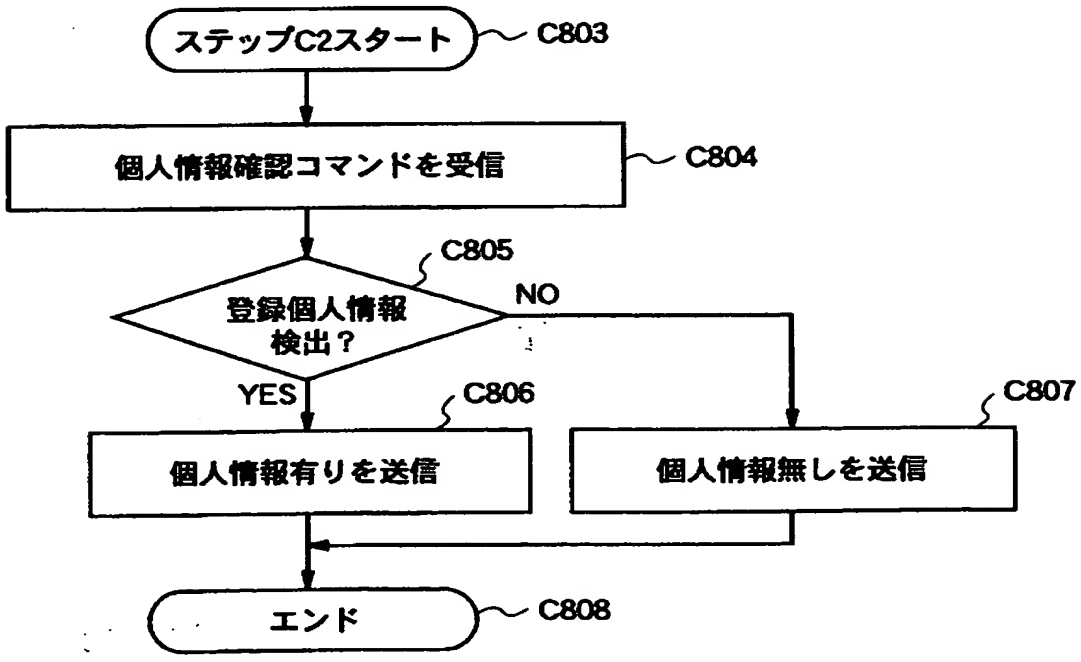
【図２３】




【図２４】



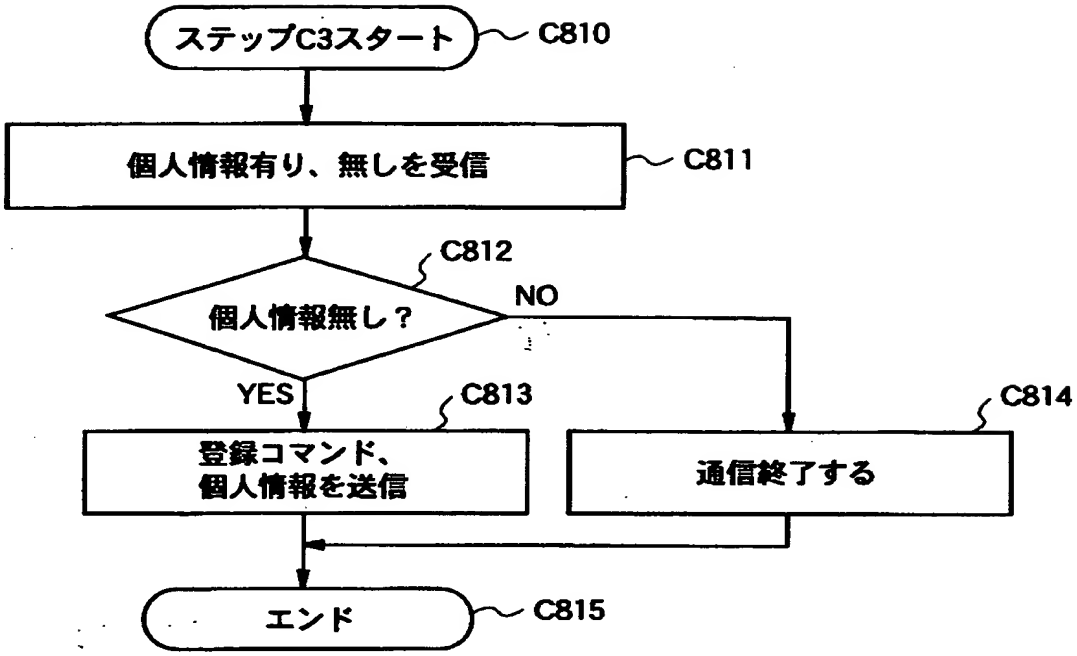

【図２５】



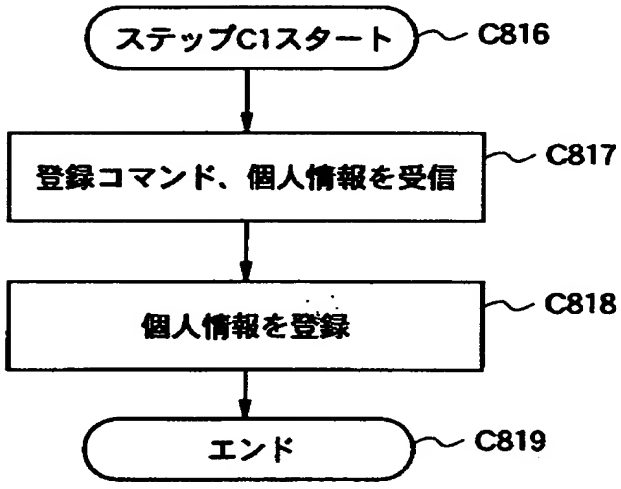


出証特２０００－３０６４３８１

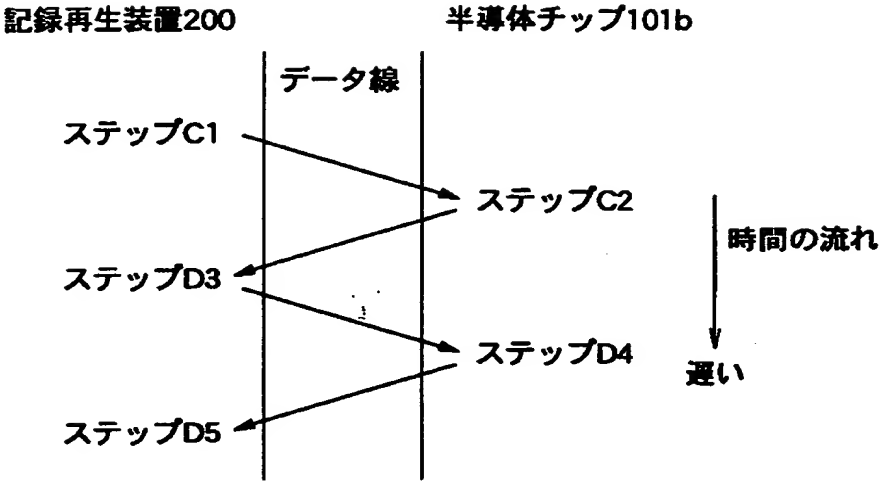
【図２６】


ステップC3スタート
C810
個人情報有り、無しを受信
C811
C812
個人情報無し？
NO
YES
C813
登録コマンド、
個人情報を送信
C814
通信終了する
エンド
C815

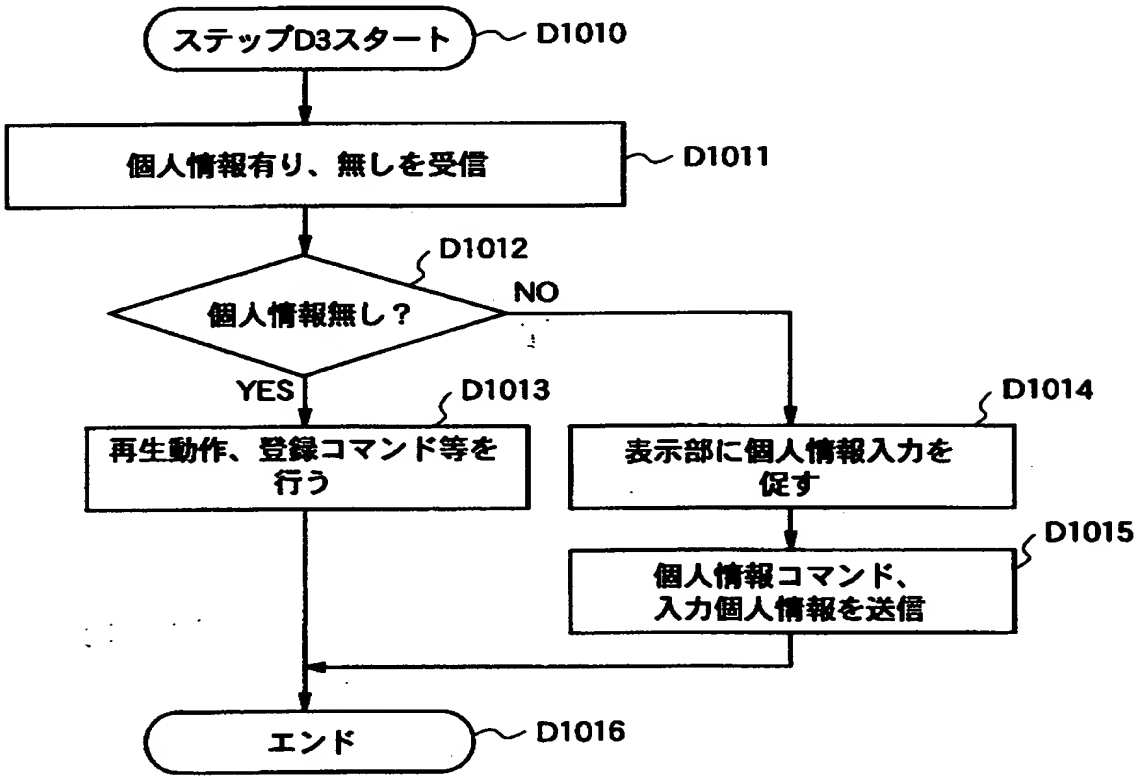
【図２７】


ステップC1スタート
C816
登録コマンド、個人情報を受信
C817
個人情報を登録
C818
エンド
C819

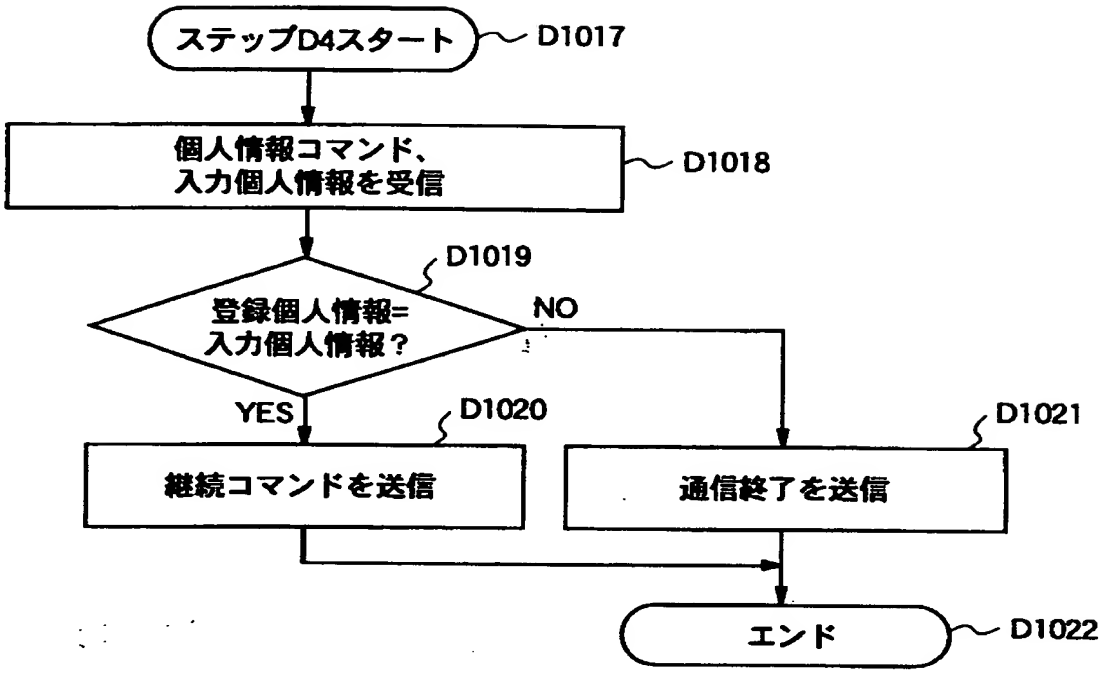
【図２８】


記録再生装置200
半導体チップ101b
データ線
ステップC1
ステップC2
ステップD3
ステップD4
ステップD5
時間の流れ
遅い

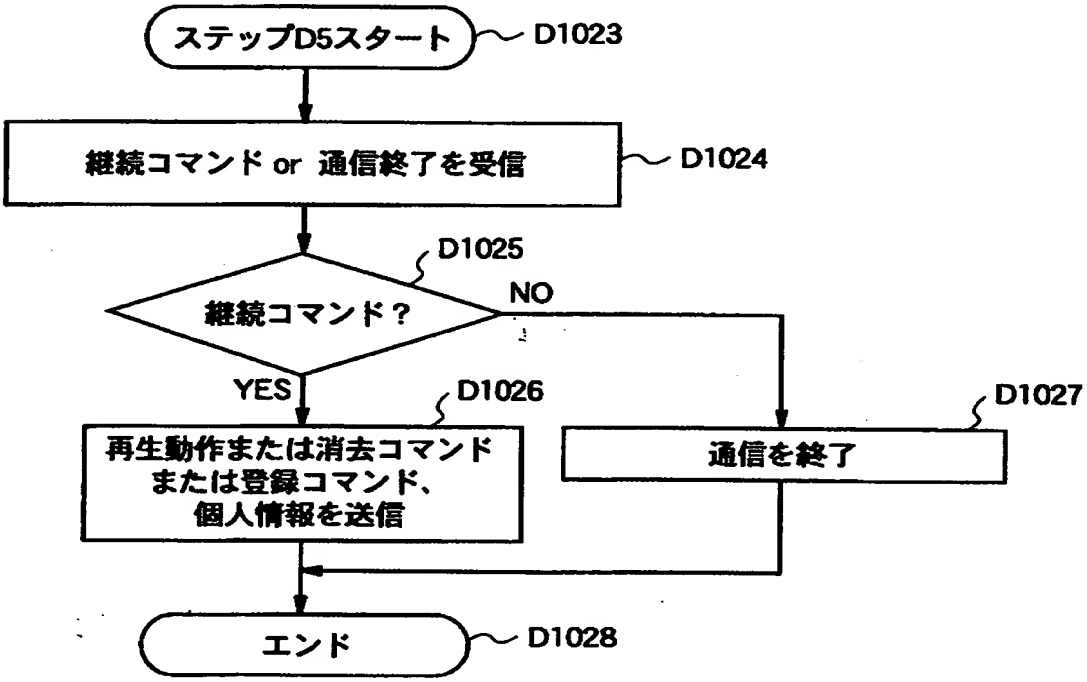
【図２９】


ステップD3スタート
D1010
個人情報有り、無しを受信
D1011
D1012
個人情報無し？
NO
YES
D1013
再生動作、登録コマンド等を行う
D1014
表示部に個人情報入力を促す
D1015
個人情報コマンド、入力個人情報を送信
エンド
D1016

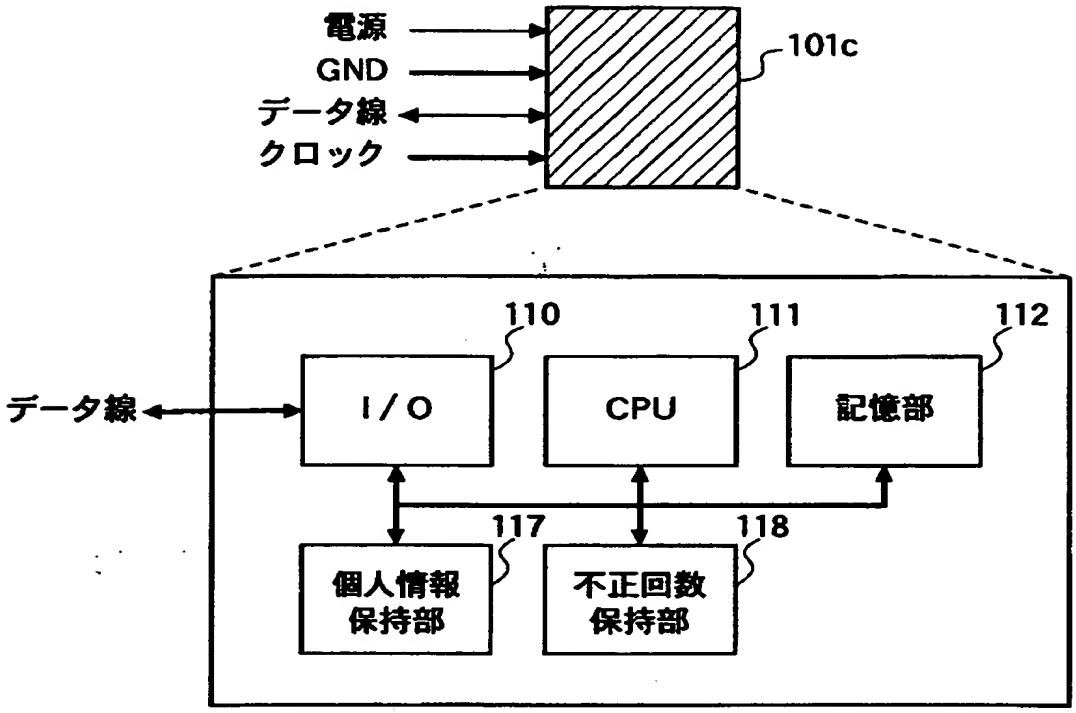
【図３０】


ステップD4スタート
D1017
個人情報コマンド、
入力個人情報を受信
D1018
D1019
登録個人情報=
入力個人情報？
NO
YES
D1020
継続コマンドを送信
D1021
通信終了を送信
エンド
D1022

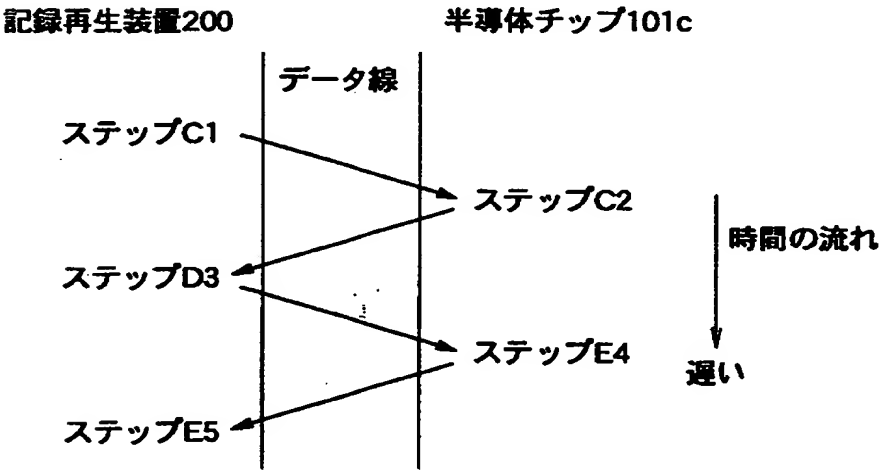
【図３１】


ステップD5スタート
D1023
継続コマンド or 通信終了を受信
D1024
D1025
継続コマンド？
NO
YES
D1026
再生動作または消去コマンド
または登録コマンド、
個人情報を送信
D1027
通信を終了
エンド
D1028

【図３２】



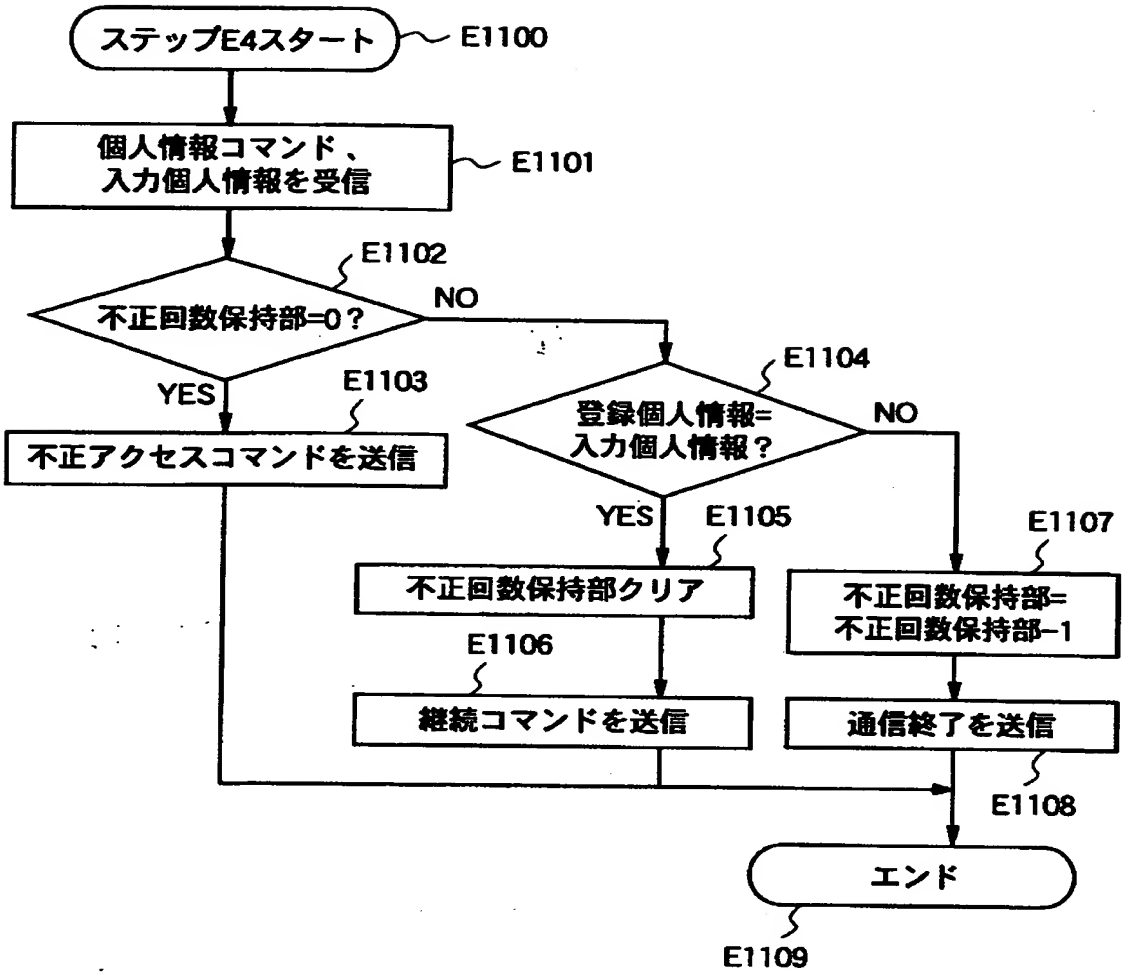

【図３３】



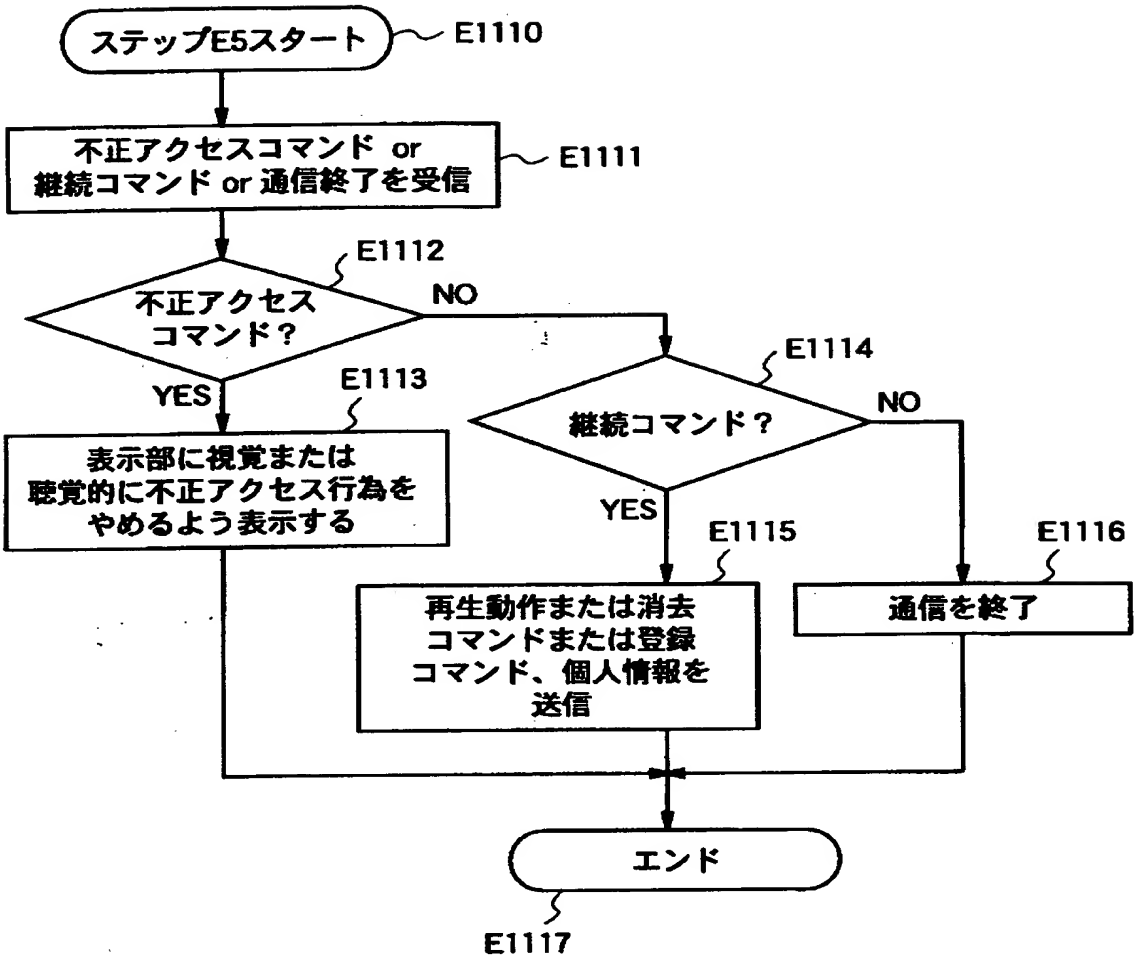


出証特２０００－３０６４３８１

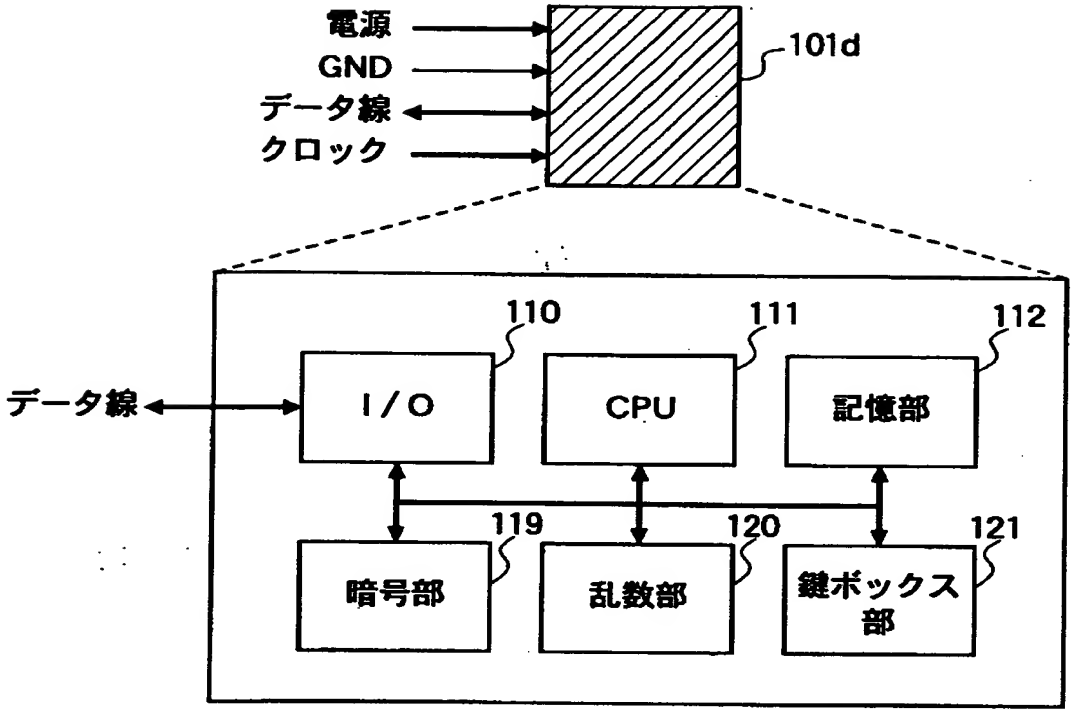
【図３４】


ステップE4スタート
E1100
個人情報コマンド、
入力個人情報を受信
E1101
E1102
不正回数保持部=0？
NO
YES
E1103
不正アクセスコマンドを送信
E1104
登録個人情報=
入力個人情報？
NO
YES
E1105
不正回数保持部クリア
E1106
継続コマンドを送信
E1107
不正回数保持部=
不正回数保持部-1
通信終了を送信
E1108
エンド
E1109

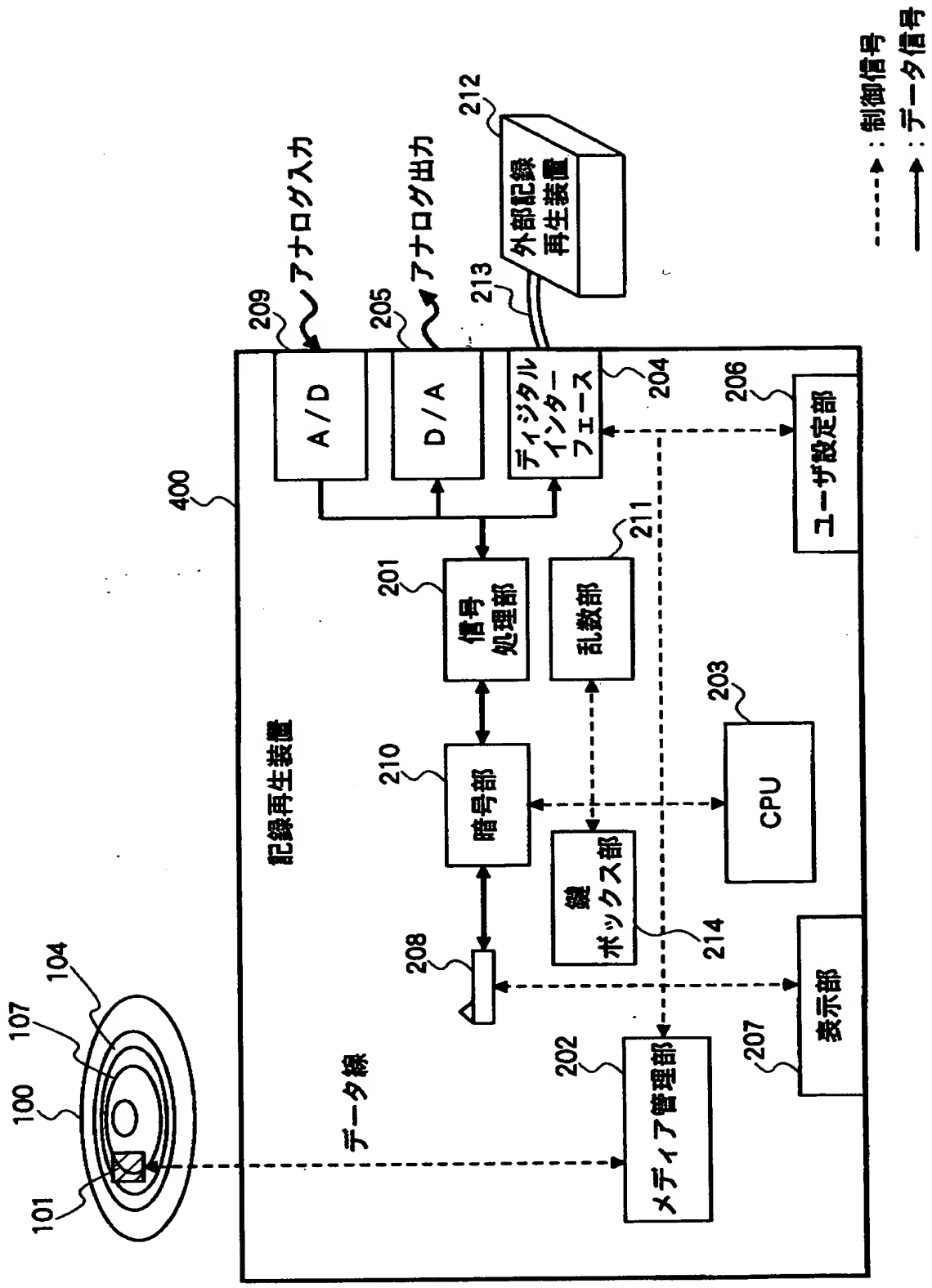
【図３５】


ステップE5スタート
E1110
不正アクセスコマンド or
継続コマンド or 通信終了を受信
E1111
E1112
不正アクセス
コマンド？
NO
YES
E1113
表示部に視覚または
聴覚的に不正アクセス行為を
やめるよう表示する
E1114
継続コマンド？
NO
YES
E1115
再生動作または消去
コマンドまたは登録
コマンド、個人情報を
送信
E1116
通信を終了
エンド
E1117

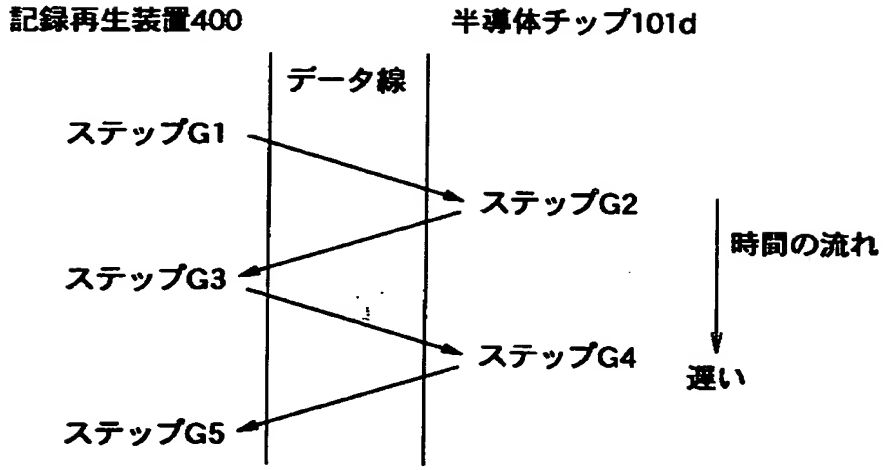
【図３６】


電源
GND
データ線
クロック
101d
データ線
I/O
CPU
記憶部
110
111
112
暗号部
乱数部
鍵ボックス部
119
120
121

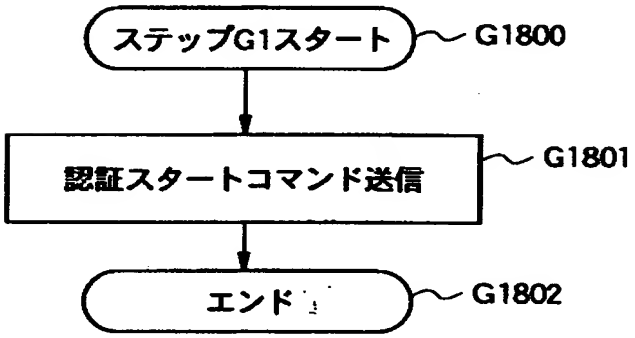
【図３７】


：制御信号
：データ信号
212
外部記録再生装置
213
209
アナログ入力
205
アナログ出力
A/D
D/A
ディジタルインターフェース
204
206
ユーザ設定部
400
211
201
信号処理部
乱数部
203
記録再生装置
210
暗号部
CPU
鍵ボックス部
214
208
表示部
207
202
メディア管理部
データ線
104
107
100
101

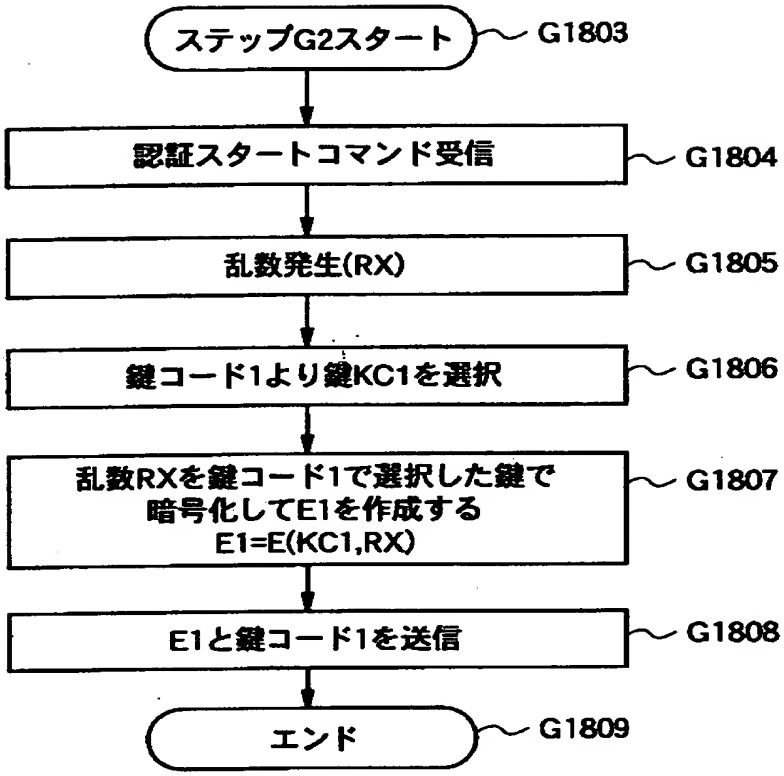
【図３８】


記録再生装置400
半導体チップ101d
データ線
ステップG1
ステップG2
ステップG3
ステップG4
ステップG5
時間の流れ
遅い

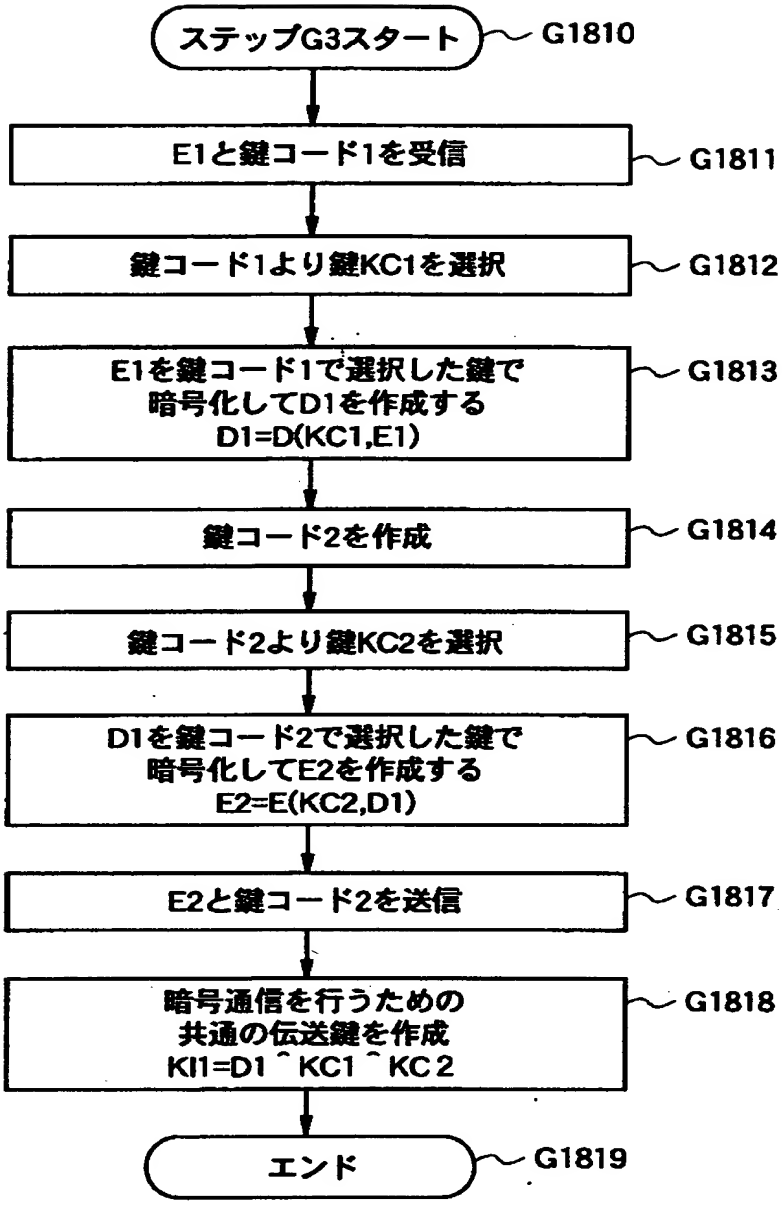
【図３９】


ステップG1スタート
G1800
認証スタートコマンド送信
G1801
エンド
G1802

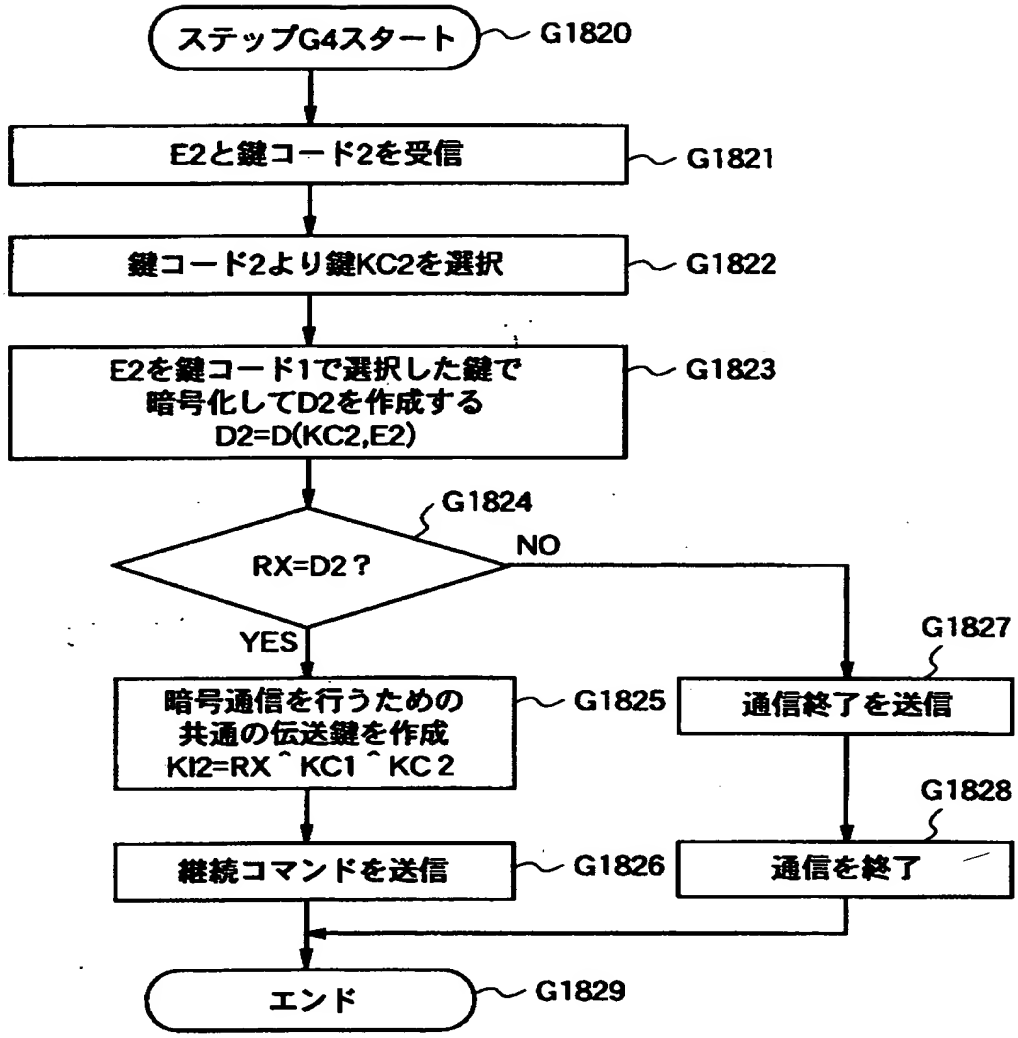
【図４０】


ステップG2スタート
G1803
認証スタートコマンド受信
G1804
乱数発生(RX)
G1805
鍵コード1より鍵KC1を選択
G1806
乱数RXを鍵コード1で選択した鍵で
暗号化してE1を作成する
E1=E(KC1,RX)
G1807
E1と鍵コード1を送信
G1808
エンド
G1809

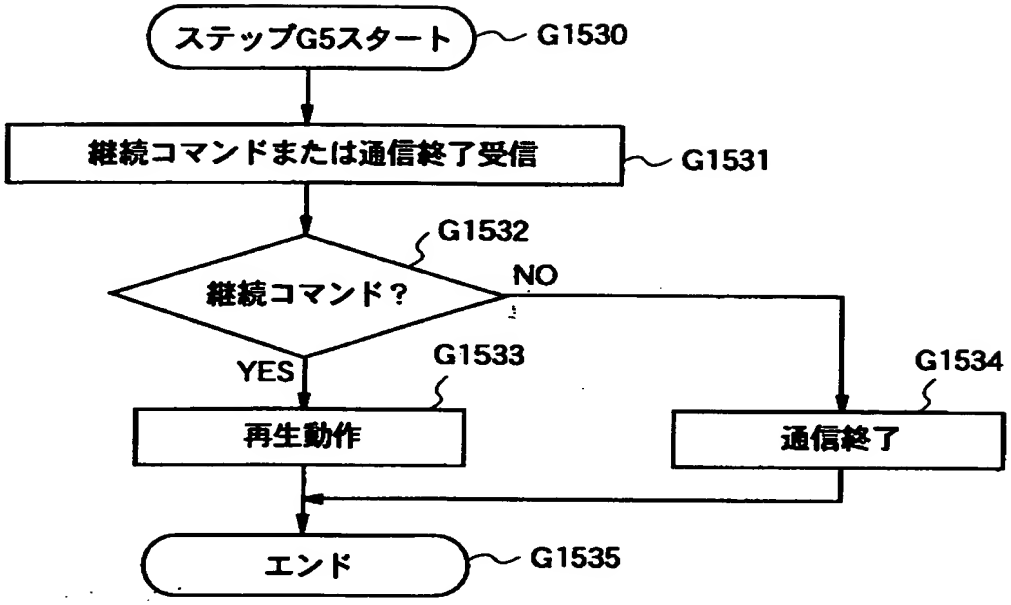
【図４１】


ステップG3スタート
G1810
E1と鍵コード1を受信
G1811
鍵コード1より鍵KC1を選択
G1812
E1を鍵コード1で選択した鍵で
暗号化してD1を作成する
D1=D(KC1,E1)
G1813
鍵コード2を作成
G1814
鍵コード2より鍵KC2を選択
G1815
D1を鍵コード2で選択した鍵で
暗号化してE2を作成する
E2=E(KC2,D1)
G1816
E2と鍵コード2を送信
G1817
暗号通信を行うための
共通の伝送鍵を作成
KI1=D1 ^ KC1 ^ KC2
G1818
エンド
G1819

【図４２】


ステップG4スタート
G1820
E2と鍵コード2を受信
G1821
鍵コード2より鍵KC2を選択
G1822
E2を鍵コード1で選択した鍵で
暗号化してD2を作成する
D2=D(KC2,E2)
G1823
G1824
RX=D2？
NO
YES
G1827
暗号通信を行うための
共通の伝送鍵を作成
KI2=RX＾KC1＾KC２
G1825
通信終了を送信
G1828
継続コマンドを送信
G1826
通信を終了
エンド
G1829

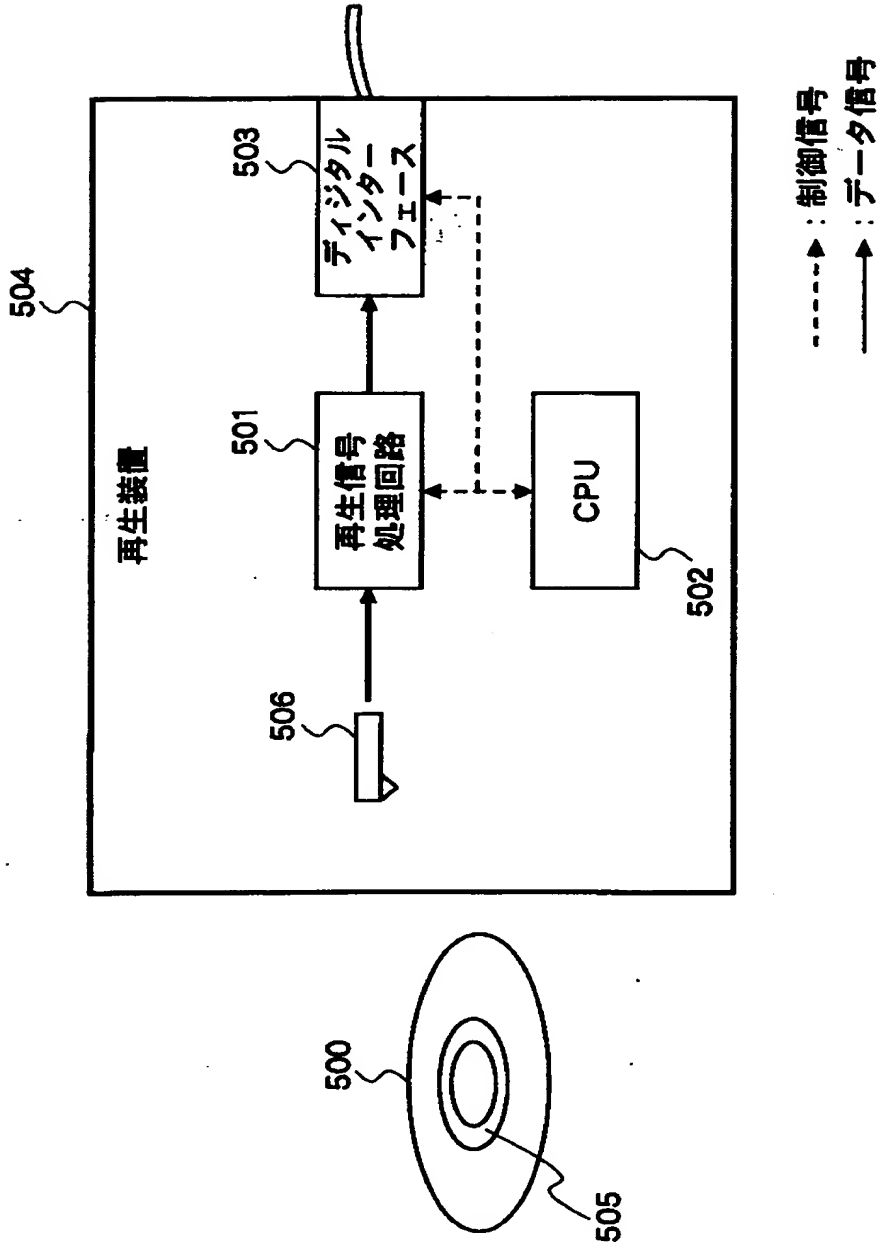
【図４３】




【図４４】

| | |
|---|---|
| Free | コピー自由 |
| Never Copy | コピー禁止 |
| One More Copy | 1回だけコピー可能 |
| No More Copy | コピー禁止<br>(One More Copyのコンテンツを別のメディアに記録する際にNo More Copyする) |

【図４５】


再生装置
504
ディジタル
インター
フェース
503
再生信号
処理回路
501
CPU
502
506
500
505
：制御信号
：データ信号

【書類名】　　要約書

【要約】

【目的】　ディスクメディアのコンテンツ情報をディジタルコピーまたはディジタル出力する場合において、信頼性の高い著作権保護を提供すること。

【解決手段】　ディスクメディア１００に内蔵した半導体ＩＣ１０１を用いて、ディスクメディア１００におけるコンテンツの再生を管理することで、ディジタルインターフェース２０４からのディジタル出力を制限する。

【選択図】　　図５

# 出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社